UNIVERSIDAD DE COSTA RICA

FACULTAD DE DERECHO

# Protección de Datos en la Convergencia de las Telecomunicaciones: El Caso de Costa Rica

TESIS PARA OPTAR POR EL GRADO DE LICENCIATURA EN DERECHO

ADRIÁN QUESADA RODRÍGUEZ

2014

Firmado digitalmente por ADRIAN QUESADA RODRIGUEZ (FIRMA)
Nombre de reconocimiento (DN): serialNumber=CPF-02-0645-0460, sn=QUESADA RODRIGUEZ, givenName=ADRIAN, c=CR, o=PERSONA FISICA, ou=CIUDADANO, cn=ADRIAN QUESADA RODRIGUEZ (FIRMA)
Fecha: 2014.07.28 21:02:46 -06'00'

UNIVERSIDAD DE COSTA RICA | ACREDITACIÓN MARCANDO JUNTOS LA DIFERENCIA

Facultad de Derecho
Área de Investigación

FACULTAD DE DERECHO

*19 de junio del 2014*
***FD-AI-422-2014***

*Dr. Alfredo Chirino Sánchez*
*Decano*
*Facultad de Derecho*

*Estimado señor:*

*Para los efectos reglamentarios correspondientes, le informo que el Trabajo Final de Graduación (categoría Tesis), del estudiante:* ***Adrián Quesada Rodríguez****, carné A75055, denominado: "Protección de Datos en la Convergencia de las Telecomunicaciones: El caso de Costa Rica" fue aprobado por el Comité Asesor, para que sea sometido a su defensa final. Asimismo, el suscrito ha revisado los requisitos de forma y orientación exigidos por esta Área y lo apruebo en el mismo sentido.*

*Igualmente, le presento a los (as) miembros (as) del Tribunal Examinador de la presente Tesis, quienes firmaron acuso de la tesis (firma y fecha) de conformidad con el Art. 36 de RTFG que indica:* ***"EL O LA ESTUDIANTE DEBERA ENTREGAR A CADA UNO DE LOS (AS) MIEMBROS (AS) DEL TRIBUNAL UN BORRADOR FINAL DE SU TESIS, CON NO MENOS DE 8 DIAS HABILES DE ANTICIPACION A LA FECHA DE PRESENTACION PUBLICA".***

***Tribunal Examinador***

| | |
|---|---|
| ***Informante*** | *Dr. Alfredo Chirino Sánchez* |
| ***Presidente*** | *Dr. Marvin Carvajal Pérez* |
| ***Secretaria (o)*** | *Dr. Jorge Córdoba Ortega* |
| ***Miembro*** | *LL.M. Federico Chacón Loaiza* |
| ***Miembro*** | *MSc. Nathalie Artavia Chavarría* |

*Por último, le informo que la defensa de la tesis es el* ***23 de julio del 2014,*** *a las 7:00 p.m. en la Sala de Conferencias, 5to. Piso, Facultad de Derecho, Sede Rodrigo Facio.*

*Atentamente,*

*Ricardo Salas Porras*
*Director*

*Ava*
*Cc: Expediente*

Teléfonos 2511-1547 Fax 2511-4089 Correo electrónico: investigacion.fd@ucr.ac.cr

San José, 16 de junio de 2014.

Señor Doctor

Ricardo Salas

Director Área de Investigación

Presente

Asunto: **Aprobación de tesis de Adrián Quesada Rodríguez**

Estimado Don Ricardo:

Por este medio, me permito comunicarle que he leído, en calidad de Director de la Investigación, la tesis elaborada por el estudiante de esta Facultad de Derecho, Adrián Quesada Rodríguez, intitulada: "Protección de Datos en la Convergencia de las Telecomunicaciones: El Caso de Costa Rica".

El señor Quesada Rodríguez ha realizado una muy informativa investigación sobre el fenómeno tecnológico de las telecomunicaciones y sus repercusiones en el derecho de la protección de datos personales, tema de indudable relevancia en el momento jurídico que vive el país.

La tesis que ha sido elaborada por el estudiante Quesada Rodríguez se ha beneficiado, positivamente, de las relaciones académicas que ha construido con autoridades internacionales en la materia a lo largo del proceso de investigación, quienes han sugerido material de trabajo y lectura que han tenido un efecto importante en la extensión y calidad de los datos e informaciones que recopila. A no dudarlo, se trata de un importante aporte a esta temática y constituye una base para investigaciones futuras que pretendan profundizar los múltiples temas abordados por don Adrián en este trabajo.

Creo, por lo anterior, que la tesis cumple a cabalidad los requisitos establecidos por la Dirección a su digno cargo, y merece ser defendida ante el Tribunal que se designe al efecto.

Sin otro particular, se suscribe,

Cordialmente,

Prof. Dr. Alfredo Chirino Sánchez
Director de la Tesis

**CARTA DE APROBACIÓN DE TESIS COMITÉ ASESOR**

**(LECTOR)**

San José, 10 de junio de 2014

Dr. Ricardo Salas Porras
Director del Área de Investigación
Facultad de Derecho
Universidad de Costa Rica
Ciudad Universitaria Rodrigo Facio, San José

Estimado Señor:

Por este medio, en mi condición de lector de tesis indico mi conformidad y aprobación para que la tesis titulada "Protección de datos en la convergencia de las telecomunicaciones: el caso de Costa Rica". Elaborada por el estudiante Adrián Quesada Rodríguez, carné A75055, sea defendida públicamente. Asimismo, hago constar por este medio que la misma cuenta con los criterios establecidos por el reglamento de trabajos finales de graduación de la Universidad de Costa Rica.

Atentamente

Dr. Marvin Carvajal Pérez

Lector de la Tesis

**CARTA DE APROBACIÓN DE TESIS COMITÉ ASESOR**

**(LECTOR)**

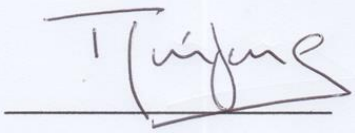
San José, 10 de junio de 2014

Dr. Ricardo Salas Porras
Director del Área de Investigación
Facultad de Derecho
Universidad de Costa Rica
Ciudad Universitaria Rodrigo Facio, San José

Estimado Señor:

Por este medio, en mi condición de lector de tesis indico mi conformidad y aprobación para que la tesis titulada "Protección de datos en la convergencia de las telecomunicaciones: el caso de Costa Rica". Elaborada por el estudiante Adrián Quesada Rodríguez, carné A75055, sea defendida públicamente. Asimismo, hago constar por este medio que la misma cuenta con los criterios establecidos por el reglamento de trabajos finales de graduación de la Universidad de Costa Rica.

Atentamente



LL.M. Federico Chacón Loaiza

Lector de la Tesis

Puntarenas, 4 de junio de 2014

Señores: Área de Investigación
Facultad de Derecho
Universidad de Costa Rica
Sede Rodrigo Facio

Estimados señores:

Por este medio hago constar que la tesis titulada: "Protección de Datos en la Convergencia de las Telecomunicaciones: El Caso de Costa Rica", propiedad de Adrián Quesada Rodríguez, carné universitario No. **A75055, y** presentada para optar por el grado académico de Licenciatura en Derecho, ha sido sometida a la revisión filológica correspondiente.

Cordialmente,

Licda. Magdalena Venegas Porras
Filóloga
Carné 10785
Cédula 6-230-116

# Dedicatoria

A mi madre, Nuria Rodríguez Gonzalo, por su cariño y sustento.

A mi padre, Walter Antillón Montealegre, por su ejemplo y dirección.

A mi abuela, Leonor Gonzalo Yuhanson, por su entrega y dedicación.

A mi novia, Vielka Arroyo Vargas, por su paciencia y dulzura.

A mi perro, Loki, por su leal compañía.

# Agradecimientos

Al Prof. Dr. Eric Alfredo Chirino Sánchez, por impulsarme a estudiar el tema y acompañar mis esfuerzos investigativos.

Al Prof. Dr. Marvin Carvajal Pérez, el Prof. Dr. Jorge Córdoba Ortega y al Prof. LL.M. Federico Chacón Loaiza, por siempre responder mis consultas y asumir la lectura de esta tesis.

A la Escuela del Sur de Gobernanza de Internet, la Sociedad del Internet de Costa Rica y la Corporación de Internet para la Asignación de Nombres y Números, por impulsar mi inclusión en la comunidad global de Gobernanza de Internet.

A la Oficina de la Comisionada de Información y Privacidad de Ontario, Canadá, por ayudarme a comprender la importancia de la Privacidad por Diseño.

A la M.Sc. Maryleana Méndez, presidente de la Junta Directiva de SUTEL y a la M.Sc. Nathalie Artavia, Directora Nacional de PRODHAB, por recibirme en sus oficinas y aclarar mis dudas.

A todas aquellas personas que me apoyaron durante estos dos largos años.

*"Cuando se disponga de medios para elaborar un registro de todos nuestros actos, y se tenga acceso a ese registro, ¿quién será capaz de autolimitarse en su uso y abuso?*
*A medida que vayamos logrando el poder de control del comportamiento humano, ¿quién decidirá cómo utilizarlo?"*
*-John Diebold*

# Índice General

**DEDICATORIA** ..... **VI**

**AGRADECIMIENTOS** ..... **VII**

**ÍNDICE GENERAL** ..... **IX**

**RESUMEN** ..... **XVIII**

**FICHA BIBLIOGRÁFICA** ..... **XX**

**INTRODUCCIÓN GENERAL** ..... **1**

**PROBLEMA E HIPÓTESIS** ..... **4**

PROBLEMA ..... 4
HIPÓTESIS ..... 5

**OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS** ..... **6**

OBJETIVO GENERAL ..... 6
OBJETIVOS ESPECÍFICOS ..... 7

**METODOLOGÍA** ..... **8**

**TÍTULO PRIMERO: MARCO TEÓRICO DE LA PROTECCIÓN DE DATOS** ..... **9**

CAPÍTULO I: INTIMIDAD, PRIVACIDAD, INFORMACIÓN Y AUTODETERMINACIÓN INFORMATIVA COMO DERECHOS HUMANOS ..... 9

*Sección I: Fundamentos Teórico-Históricos de la Protección de la Personalidad por los Derechos Humanos* ..... *10*

Breve Introducción Histórica ..... 11
Antigüedad ..... 12
Grecia Clásica ..... 14
Roma ..... 16
Edad Media ..... 19
Del Renacimiento hasta el Siglo XVII ..... 21
Siglo XVIII ..... 23
Siglo XIX hasta Siglo XX ..... 26
El Desarrollo de las Tecnologías de la Información y la Comunicación en los Siglos XX y XXI y el Surgimiento de la "Personalidad Virtual" ..... 31
Derechos Humanos, Derechos Fundamentales y Derechos de la Personalidad ..... 35
Derechos Humanos ..... 36
Definición ..... 36
Fundamentos ..... 38
Principios ..... 39
Clasificaciones ..... 41
Derechos Fundamentales o Garantías Individuales ..... 46
Definición ..... 46
Fundamentos ..... 48
Características ..... 49
Derechos de la Personalidad ..... 50
Definición ..... 51
Fundamentos ..... 53
Características ..... 56
Clasificaciones ..... 57

Síntesis de la Primera Sección ..... 61
*Sección II: Intimidad, Privacidad, Información y Autodeterminación Informativa como Bienes Jurídicos Tutelados en el Derecho Nacional e Internacional ..... 67*
Derecho a la Intimidad y el "Right to Privacy" Anglosajón ..... 68
El Derecho a la Intimidad ..... 69
Fundamentos y Definición del Derecho a la Intimidad ..... 69
Naturaleza Jurídica y Características del Derecho a la Intimidad ..... 72
Elementos del Derecho a la Intimidad ..... 76
Vida Privada ..... 77
Privacidad ..... 79
Autonomía de la Voluntad ..... 80
Distinción entre lo Público y lo Privado ..... 82
Limitaciones del Derecho a la Intimidad ..... 84
Manifestaciones del Derecho a la Intimidad en el Derecho Nacional e Internacional ..... 85
La Intimidad como Bien Jurídico Tutelado en el Ámbito Nacional ..... 85
Manifestaciones del Derecho a la Intimidad en el Plano Internacional ..... 88
Declaración Universal de Derechos Humanos ..... 88
Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales ..... 89
Pacto Internacional de Derechos Económicos, Sociales y Culturales ..... 90
Pacto Internacional de Derechos Civiles y Políticos ..... 90
Convención Americana sobre Derechos Humanos ..... 91
El Derecho a la Privacidad (el "Right to Privacy" Anglosajón) ..... 92
Fundamentos del Derecho a la Privacidad. ..... 93
El "Right to Privacy" en Estados Unidos de América ..... 95
Tratamiento Jurisprudencial en el Common Law ..... 96
Actos de intrusión que perturban el retiro o soledad del individuo ..... 96
Divulgación pública de hechos privados embarazosos sobre el individuo ..... 97
Publicidad que coloca al individuo bajo una luz falsa ante el público ..... 99
Apropiación de la imagen o identidad de una persona para derivar algún beneficio ..... 100
Derecho Constitucional ..... 101
Derecho Codificado ..... 102
Derecho a la Información y Derecho de Autodeterminación Informativa ..... 102
El Derecho a la Información ..... 103
Fundamentos y Definición del Derecho a la Información ..... 105
Información Privada ..... 107
Información Pública ..... 108
Información de Interés General ..... 109
Definiciones de Derecho a la Información ..... 110
Naturaleza Jurídica y Principios del Derecho a la Información ..... 111
Principios del Derecho a la Información ..... 112
Principios Ideales del Derecho a la Información ..... 113
Principios Relacionados con el Derecho al Acceso a la Información, Vigentes en el Marco del Derecho Público Costarricense ..... 115
Elementos del Derecho a la Información ..... 117
Problemática del Derecho a la Información ..... 120
El Derecho de Autodeterminación Informativa ..... 122
Definición y Fundamentos del Derecho de Autodeterminación Informativa ..... 123
Naturaleza Jurídica y Características del Derecho de Autodeterminación Informativa ..... 127
Elementos y Principios del Derecho de Autodeterminación Informativa ..... 131
Síntesis de la Segunda Sección ..... 137
CAPÍTULO II: LA PROTECCIÓN DE DATOS PERSONALES, EVOLUCIÓN Y FUNDAMENTOS IUSINFORMÁTICOS FRENTE A LA CONVERGENCIA DE LAS TELECOMUNICACIONES ..... 143

*Sección I: Surgimiento y Fundamentos de la Protección de los Datos Personales desde la Perspectiva Iusinformática* ..... *144*
Surgimiento de la Perspectiva Iusniformática: el Derecho Informático y los Orígenes de la Protección de Datos ..... 145
Breve Introducción Histórica y Contextual ..... 145
El Surgimiento de las Bases de Datos ..... 145
Las Técnicas de Seguridad de la Información ..... 148
El Derecho Informático y la Perspectiva Iusinformática ..... 154
Adopción Legal de la Protección de Datos Personales ..... 158
Caracterización de la Protección de Datos desde la Perspectiva Iusinformática ..... 162
Definición Terminológica ..... 163
Problemática del Tratamiento de los Datos Personales ..... 165
Objetivos de la Protección de Datos Personales ..... 168
Sujetos de la Protección de Datos Personales ..... 171
Sujeto Activo ..... 171
Sujeto Pasivo ..... 177
Objeto de la Protección de Datos Personales ..... 179
Breve Tipología de los Datos Personales ..... 182
Principios Legales Generalmente Aplicables al Objeto de la Protección de Datos ..... 187
Las Etapas del Tratamiento de los Datos Personales - Principios Específicamente Involucrados . 191
Etapa de Recopilación de los Datos (Etapa de Input) ..... 192
Etapa de Tratamiento de los Datos ..... 196
Etapa de Transmisión o Utilización de los Datos o Resultados (Etapa de Output) ..... 200
Síntesis de la Primera Sección ..... 203
*Sección II: Telecomunicaciones Convergentes y Problemas Emergentes de la Protección de Datos* ..... *208*
Fundamentos de Telecomunicaciones ..... 210
Las Tres Olas Tecnológicas ..... 215
La Primera Ola: De las Telecomunicaciones Analógicas a las Telecomunicaciones Digitales. ..... 215
Digitalización de Redes ..... 216
Desarrollo de la Informática ..... 218
Conmutación de Paquetes ..... 220
La Segunda Ola: El Surgimiento de las Redes de Nueva Generación ..... 225
La Tercera Ola: Nuevas Aplicaciones de las TICs ..... 228
La Convergencia de las Telecomunicaciones ..... 229
La Convergencia de las Telecomunicaciones y sus Efectos en los Modelos de Regulación Nacionales e Internacionales ..... 233
Efectos en el Plano Nacional ..... 233
Efectos en el Plano Internacional: los Modelos de Gobernanza Multilateral y el Surgimiento del Modelo de Gobernanza por Múltiples Interesados ..... 235
La Unión Internacional de las Telecomunicaciones y el Modelo de Gobernanza Multilateral ..... 236
La Gobernanza de Internet y el Modelo de Múltiples Interesados ..... 241
Problemas Emergentes de la Protección de Datos Frente a la Convergencia de las Telecomunicaciones .. 249
Proliferación de Cookies ..... 251
Elaboración de Perfiles y Redes Sociales ..... 255
Traición por Datos de Localización ..... 261
Transferencias Internacionales de Datos Personales ..... 264
Violaciones a la Autodeterminación Informativa por otros Estados ..... 274
Síntesis de la Segunda Sección ..... 279

**TÍTULO SEGUNDO: LA PROTECCIÓN DE DATOS EN EL ÁMBITO INTERNACIONAL. FUNCIONAMIENTO Y NORMATIVA RELEVANTE PARA LAS TELECOMUNICACIONES CONVERGENTES ..... 289**

CAPÍTULO I: MARCOS LEGALES REPRESENTATIVOS EN MATERIA DE PROTECCIÓN DE DATOS EN EL DERECHO COMPARADO ..... 289
*Sección I: Modelo Europeo y Sistema Norteamericano ..... 290*
Marco Europeo de Protección de Datos Personales ..... 290
Marco Legal Fundamental ..... 292
Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01) ..... 292
Tratado de la Unión Europea ..... 293
Tratado sobre el Funcionamiento de la Unión Europea ..... 296
Convenio 108 del Consejo de Europa del 28 de enero de 1981 ..... 297
Protocolo adicional al Convenio 108 del Consejo de Europa del 8 de noviembre de 2001 ..... 299
Directivas: ..... 300
Directiva 95/46/EC ..... 300
Directiva 2002/58/EC ..... 303
Directiva 2006/24/EC ..... 306
Decisión Marco 2008/977/JHA ..... 308
Directiva 2009/136/EC ..... 312
Regulación ..... 314
Regulación (EC) 45/2001 ..... 314
Reformas Propuestas ..... 315
Propuesta de Reglamento General de la Protección de Datos 2012/0011(COD) ..... 316
Propuesta de Directiva del Parlamento Europeo y del Consejo 2012/0010(COD) ..... 319
Modelo Estadounidense ..... 322
Legislación Federal Relevante ..... 323
Americans with Disabilities Act of 1990 ..... 323
Bank Secrecy Act of 1970 ..... 324
Cable Communications Privacy Act of 1984 ..... 325
Children's Internet Protection Act of 2000 ..... 326
Children's Online Privacy Protection Act of 1998 ..... 327
Computer Fraud and Abuse Act of 1984 ..... 329
Communications Assistance for Law Enforcement Act of 1994 ..... 330
Computer Matching and Privacy Protection Act of 1998 ..... 331
Consumer Credit Reporting Reform Act of 1996 ..... 333
Drivers Privacy Protection Act of 1994 ..... 334
Electronic Communications Privacy Act of 1984 ..... 335
Electronic Freedom of Information Act of 1996 ..... 336
Electronic Funds Transfer Act of 1978 ..... 337
Equal Credit Opportunity Act of 1974 ..... 338
Fair and Accurate Credit Transactions Act of 2003 ..... 339
FACTA Disposal Rule of 2005 ..... 340
Fair Credit Reporting Act of 1970 ..... 340
Fair Debt Collection Practices Act of 1996 ..... 342
Family Education Rights and Privacy Act of 1974 ..... 342
Federal Trade Commission Act of 1938 ..... 343
Financial Services Regulatory Relief Act of 2006 ..... 344
Gramm-Leach-Bliley Financial Modernization Act of 1999 ..... 345
Health Insurance Portability Act of 1996 ..... 346
Health Information Technology for Economic and Clinical Health Act of 2009 ..... 347
Identity Theft and Assumption Deterrence Act of 1998 ..... 348
Privacy Act of 1974 ..... 349
Privacy Protection Act of 1980 ..... 351
Right to Financial Privacy Act ..... 352
Sarbanes-Oxley Act of 2002 ..... 352
Telecommunications Act of 1996 ..... 353

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ..... 354
Video Privacy Protection Act of 1988 ..... 355
La Carta de Derechos de Privacidad del Consumidor y el Marco de Protección de la Privacidad y la Innovación en la Economía Global Digital ..... 356
Síntesis de la Primera Sección ..... 360
*Sección II: Modelos Nacionales ..... 367*
Sistemas Legales Nacionales Basados en el Habeas Data ..... 368
Brasil ..... 370
Paraguay ..... 375
Perú ..... 378
Argentina ..... 383
Colombia ..... 387
Adopción Nacional de Normativa Especializada ..... 391
España ..... 392
Canadá ..... 395
México ..... 397
Japón ..... 401
China ..... 404
Síntesis de la Segunda Sección ..... 409
*Sección III: Sistemas y Estándares Internacionales para la Protección de Datos ..... 417*
Sistemas Internacionales ..... 419
Convenio 108 del Consejo de Europa del 28 de Enero de 1981 para la Protección de los Individuos con Respecto al Procesamiento Automatizado de Datos Personales de 1980 y su Protocolo Adicional de 2001 ..... 420
El Programa de Safe Harbor ..... 420
Protección Adecuada Según Estándares Europeos ..... 425
Guías de la Organización para la Cooperación y el Desarrollo Económico ..... 427
Red Iberoamericana de Protección de Datos ..... 430
Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico ..... 434
Resoluciones y Declaraciones de las Conferencias Internacionales de Autoridades de Protección de Datos y Privacidad ..... 439
Declaración de Varsovia sobre la "Appification" de la Sociedad – La Privacidad: una Brújula para un Mundo en Turbulencia ..... 440
Resolución sobre el Futuro de la Privacidad ..... 441
Resolución sobre la Computación en la Nube ..... 441
Declaración de Uruguay sobre la Creación de Perfiles ..... 442
Resolución sobre Privacidad por Diseño ..... 443
Resolución de Madrid sobre Estándares Internacionales para la Protección de los Datos Personales y la Privacidad ..... 444
Propuesta de Resolución sobre Protección a la Privacidad en Redes Sociales ..... 444
Resolución sobre el Proyecto de Norma ISO para la Privacidad ..... 446
Soluciones Técnicas Internacionales ..... 446
Estándares Internacionales ..... 447
RFCs de la Internet Engineering Task Force ..... 448
Estándares ISO de la serie 27000 ..... 451
Estándar ISO 29100 ..... 453
Estándar ISO 22307 ..... 455
Protocolos ..... 456
Protocolo P3P ..... 457
Protocolo Do Not Track ..... 458
Privacidad por Diseño ..... 459
Síntesis de la Tercera Sección ..... 462

**TÍTULO TERCERO: LA PROTECCIÓN DE DATOS EN COSTA RICA: UN PROYECTO INCOMPLETO ..... 469**

CAPÍTULO I: MARCO ADMINISTRATIVO Y REGULATORIO DE LAS TELECOMUNICACIONES Y LA PROTECCIÓN DE DATOS PERSONALES EN COSTA RICA ..... 469

*Sección I: El Estado Actual de las Telecomunicaciones en Costa Rica ..... 470*

Breve Introducción Histórica de las Telecomunicaciones en Costa Rica ..... 470

Entes Nacionales Encargados de la Regulación de las Telecomunicaciones y de la Protección de Datos Personales ..... 477

Poder Ejecutivo ..... 478

Presidente de la República de Costa Rica ..... 478

Ministerios ..... 480

Ministerio de Ciencia, Tecnología y Telecomunicaciones ..... 480

Viceministerio de Telecomunicaciones ..... 484

Otros Ministerios Relacionados con el Sector Telecomunicaciones ..... 486

Ministerio de Educación Pública ..... 487

Ministerio de Salud ..... 488

Ministerio de Planificación Nacional y Política Económica ..... 490

Ministerio de Cultura, Juventud y Deportes ..... 491

Ministerio de Hacienda ..... 491

Autoridades Administrativas y Regulatorias ..... 492

Autoridad Reguladora de los Servicios Públicos ..... 494

Superintendencia de Telecomunicaciones ..... 495

Agencia de Protección de Datos de los Habitantes ..... 499

Operadores de Redes de Telecomunicaciones y Proveedores de Servicios ..... 501

Síntesis de la Primera Sección ..... 506

*Sección II: Marco Regulatorio Vigente en Costa Rica en Materia de Telecomunicaciones y Protección de Datos Personales ..... 509*

Marco Regulatorio Vigente en Materia de Telecomunicaciones ..... 510

Tratados Internacionales Ratificados por la República de Costa Rica en Materia de Telecomunicaciones ..... 511

Convención Internacional de Telecomunicaciones ..... 511

Constitución y Convención de la Unión Internacional de las Telecomunicaciones ..... 512

Tratado Centroamericano de Telecomunicaciones y su Protocolo ..... 515

Acuerdo Relacionado con la Organización Internacional de Telecomunicaciones por Satélite ..... 515

Convención Internacional de Telecomunicaciones Marítimas por Satélite ..... 516

Tratado Centroamericano de Libre Comercio e Integración Económica ..... 516

Acuerdo Marco de Cooperación entre las Repúblicas de Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá y la Comunidad Económica Europea. ..... 517

Declaración Conjunta entre los Gobiernos de Canadá y Costa Rica sobre Comercio Electrónico Global ..... 518

Tratado de Libre Comercio entre Estados Unidos, Centroamérica y República Dominicana ..... 520

Normativa Nacional en Materia de Telecomunicaciones ..... 521

Ley Nº 8660 "Ley de Fortalecimiento y Modernización de las Entidades Públicas" ..... 522

Reglamento al Título II de la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones ..... 525

Ley Nº 8642 "Ley General de Telecomunicaciones" ..... 527

Reglamento a la Ley General de Telecomunicaciones ..... 531

Ley Nº 7566 "Ley de Creación del Sistema de Emergencias 911" ..... 532

Ley Nº 7593 "Ley de la Autoridad Reguladora de Servicios Públicos" ..... 533

Marco Regulatorio Vigente en Materia de Protección de Datos Personales ..... 534

Normativa Internacional Vigente para la República de Costa Rica en Materia de Protección de Datos Personales ..... 534

Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional ..... 534

Convención Interamericana sobre Extradición ..... 537

Declaración de La Antigua sobre Datos Personales ..... 537
Estatuto de Roma de la Corte Penal Internacional ..... 539
Acuerdo de Cooperación Ambiental entre el Gobierno de Costa Rica y el Gobierno de Canadá ..... 539
Acuerdo entre el Gobierno de la República de Costa Rica y el Gobierno de la República Francesa, Relativo a la Readmisión de Personas en Situación Irregular ..... 540
Acuerdo de Diálogo Político y Cooperación entre la Comunidad Europea y sus Estados Miembros y las Repúblicas de Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá ..... 542
Acuerdo y Protocolo para el Intercambio de Información en Materia Tributaria con el Reino de los Países Bajos. ..... 543
Convención Internacional para la Protección de todas las Personas contra las Desapariciones Forzadas ..... 547
100 Reglas de Brasilia sobre Acceso a la Justicia de las Personas en Condición de Vulnerabilidad ..... 549
Reglas de Heredia sobre Difusión de Información Judicial ..... 550
Protocolo Facultativo de la Convención sobre los Derechos del Niño Relativo a la Venta de Niños, la Prostitución Infantil y Utilización de Niños en la Pornografía ..... 554
Normativa Nacional Relevante para la Protección de Datos Personales ..... 555
Tratamiento Histórico Jurisprudencial de la Protección de Datos Personales en Costa Rica ..... 557
Etapa de Reconocimiento Inconsciente ..... 559
Resolución Nº 2609-91 ..... 559
Resolución Nº 2680-94 ..... 559
Etapa de Negación ..... 560
Sentencia Nº 476-91 ..... 560
Sentencia Nº 2256-95 ..... 561
Etapa de Reconocimiento Casuístico ..... 561
Sentencia Nº 2805-98 ..... 562
Sentencia Nº 8218-98 ..... 562
Etapa de Doctrina Jurisprudencial Genérica ..... 563
Voto Nº 4154-97 ..... 564
Resolución Nº 5802-99 ..... 565
Voto Nº 1345-98 ..... 566
Voto Nº 754-02 ..... 567
Etapa de Doctrina Jurisprudencial Específica ..... 567
Sentencia Nº 8996-02 ..... 568
Sentencia Nº 2004-12239 ..... 568
Sentencia Nº 2007-10114 ..... 568
Etapa de Remisión de Asuntos de Autodeterminación Informativa a la PRODHAB ..... 569
Sentencia Nº 2013-15183 ..... 569
Leyes ..... 570
Ley Nº 63 “Código Civil” ..... 570
Ley Nº 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales ..... 571
Ley Nº 7975 “de Información No Divulgada” ..... 578
Ley Nº 4573 "Código Penal" ..... 579
Ley Nº 9048 “Reforma de la Sección VIII, Delitos Informáticos y Conexos, del título VII del Código Penal” ..... 581
Ley Nº 9135 “Reforma de los artículos 196, 196 bis, 230, 293, y 295 y adición del artículo 167 bis al Código Penal” ..... 584
Ley Nº 7425 “sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones” ..... 585
Ley Nº 8754 contra la Delincuencia Organizada ..... 587
Ley Nº 6227 “Ley General de la Administración Pública” ..... 588
Ley Nº 17 “Ley Constitutiva de la Caja Costarricense del Seguro Social” ..... 589
Ley Nº 9162 “Expediente Digital Único de Salud” ..... 591
Ley Nº 4755 “Código de Normas y Procedimientos Tributarios” ..... 593
Ley Nº 3284 “Código de Comercio” ..... 594

Ley Nº 7732 “Ley Reguladora del Mercado de Valores” ..... 595
Ley Nº 7558 “Ley Orgánica del Banco Central de Costa Rica” ..... 596
Ley Nº 8131 “Ley de la Administración Financiera de la República y Presupuestos Públicos” ..... 597
Ley Nº 8656 “Ley Reguladora del Contrato de Seguros” ..... 598
Reglamentos ..... 599
Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales ..... 599
Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones ..... 604
Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones ..... 609
Reglamento de Acceso Universal, Servicio Universal y Solidaridad ..... 615
Reglamento de Personas Refugiadas ..... 616
Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor N° 7472 ..... 617
Reglamento sobre el Registro Único de Personas Beneficiarias ..... 617
Otra Normativa Relevante ..... 618
Directriz del Ministerio de Justicia y Paz del 04 de abril de 2014 ..... 618
Resolución RCS-303-2012 SUTEL “Disposiciones complementarias, técnicas, económicas y administrativas para la implementación y operación del sistema integral de portabilidad numérica en Costa Rica” ..... 618
Acuerdo 014-077-2012 SUTEL sobre Procedimiento de Comunicaciones no Solicitadas ..... 619
Decreto Ejecutivo Nº 46-H-MICITT sobre uso de soluciones de cómputo en la nube sobre otro tipo de arquitectura ..... 623
Documento N-2-2007-CO-DFOE "Normas técnicas para la gestión y el control de las Tecnologías de Información" ..... 625
Política Judicial Dirigida al Mejoramiento del Acceso a la Justicia de las Niñas, Niños, y Adolescentes en Costa Rica ..... 626
Regulaciones en cuanto a la Transferencia de Información Personal de Clientes conforme Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales ..... 627
Directriz para Reducir la Revictimización de Niños, Niñas y Adolescentes en Condición de Discapacidad en Procesos Judiciales ..... 628
Código de Ética de las y los Profesionales en Comunicación ..... 628
Síntesis de la Segunda Sección ..... 630
CAPÍTULO II: PROTECCIÓN DE DATOS PERSONALES EN LAS TELECOMUNICACIONES CONVERGENTES, ¿UNA REALIDAD EN COSTA RICA? ..... 640
*Sección I: Análisis de la Protección de Datos en Costa Rica Frente al Derecho Comparado, ¿Cuenta Nuestro País con una Protección Adecuada?* ..... *642*
Manifestación de los Principios y Derechos Relativos a la Autodeterminación Informativa y la Protección de Datos Personales en el Marco Normativo Costarricense ..... 644
Principios ..... 645
Derechos Subjetivos ..... 665
Técnicas y Herramientas de Protección de Datos en el Contexto Legal Costarricense ..... 666
Técnicas de Seguridad de la Información ..... 667
Protocolos de Seguridad de la Información ..... 668
Registro de Incidencias ..... 669
Control de Acceso, Identificación y Autenticación ..... 670
Gestión de Soportes y Documentos ..... 671
Herramientas de Control de Transferencias ..... 672
Procesos de Actualización ..... 673
Contratos y Cláusulas Modelo de Protección de Datos ..... 674
Buenas Prácticas Corporativas ..... 676
Autorregulación Vinculante ..... 677
Privacidad por Diseño ..... 677
Ombudsman Corporativo/Institucional para la Protección de Datos Personales ..... 678

Convenios Interinstitucionales ..... 679
Referencias a Estándares Internacionales y Protocolos Técnicos ..... 680
Capacidad de reacción frente a la convergencia de las telecomunicaciones ..... 681
Proliferación de Cookies ..... 682
Un Breve Experimento: Detección de la Información Obtenida por Medio de Cookies en el Caso Costarricense ..... 682
Las cookies y el marco normativo costarricense ..... 689
Elaboración de Perfiles y Redes Sociales ..... 691
Traición por Datos de Localización ..... 695
Transferencias Internacionales de Datos Personales ..... 697
Violaciones a la Autodeterminación Informativa por otros Estados ..... 702
Ubicación de Costa Rica frente a los Sistemas Internacionales Estudiados ..... 704
Síntesis de la Primera Sección ..... 713
*Sección II: Recomendaciones* ..... *723*
Medidas Necesarias a Corto Plazo ..... 723
Medidas Necesarias a Mediano Plazo ..... 736
Cambios Necesarios a Largo Plazo ..... 747
Síntesis de la Segunda Sección ..... 750

**CONCLUSIONES GENERALES ..... 758**

**BIBLIOGRAFÍA ..... 763**

**ANEXOS ..... 821**

ANEXO 1 ..... 822
ANEXO 2 ..... 823
ANEXO 3 ..... 824
ANEXO 4 ..... 825
ANEXO 5 ..... 826
ANEXO 6 ..... 827
ANEXO 7 ..... 828
ANEXO 8 ..... 830
ANEXO 9 ..... 832
ANEXO 10 ..... 838

## Resumen

A lo largo de la presente investigación se ha analizado la protección de datos personales frente a la convergencia de las telecomunicaciones en Costa Rica, tema de vital importancia en el contexto generado por la reciente apertura del sector telecomunicaciones a la competencia y la creciente inclusión de nuestro país en la sociedad global de la información.

Fundamentalmente, esta investigación ha procurado analizar con profundidad la implicancia de la protección de datos personales en el ámbito de los servicios de información y de telecomunicaciones, de tal manera que se comprendan las ramificaciones y efectos derivados de la convergencia tecnológica y se genere una realimentación a partir del estudio de los modelos técnicos y regulatorios que tutelan los datos personales en el ámbito nacional y el internacional.

Para lograr este objetivo, se partió de tres hipótesis fundamentales, a saber:

1) La dependencia de los sistemas de telecomunicaciones convergentes en el intercambio a gran escala de información, aunada con la inexistencia de un consenso internacional sobre qué datos pueden ser tratados, retenidos y transmitidos, implica para los usuarios un constante estado de vulnerabilidad ante entes públicos y privados, quienes se encuentran interesados por igual en obtener y tratar sus informaciones sensibles.

2) El que nuestro país no se encuentre adscrito a un sistema internacional dirigido a la protección de datos personales, representa un límite a la capacidad del usuario costarricense de tecnologías convergentes de telecomunicaciones para salvaguardar sus derechos de privacidad y autodeterminación informativa más allá de los límites jurisdiccionales de su país.

3) El sistema actualmente implementado por el marco normativo nacional se encuentra limitado para defender los derechos de sus ciudadanos ante los retos planteados por la convergencia de las telecomunicaciones y la globalización de los servicios de información. Pese ser relativamente novedosa, la normativa costarricense no solo presenta errores y omisiones, sino que no logra alcanzar las tendencias y

estándares implementados por los principales modelos regulatorios internacionales en materia de protección de datos.

Con miras a demostrar estas hipótesis, esta investigación ha seguido un modelo híbrido de metodología. Mediante la integración del método documental deductivo con el método comparativo se analizará el tema desde sus elementos más generales hasta enfocarse en algunos de los problemas más específicos. Asimismo, este método permitirá realizar comparaciones fundadas en los sistemas más representativos en el plano internacional, con miras a encontrar soluciones aplicables al plano nacional.

Gracias al cumplimiento de los objetivos planteados, la investigación ha confirmado las hipótesis planteadas y ha permitido concluir que:

- La convergencia de las telecomunicaciones afecta directamente a los habitantes de Costa Rica, quienes se mantienen en constante vulnerabilidad dada la limitada protección brindada por nuestro sistema de protección de datos.
- La existencia de tan amplia diversidad normativa en el plano internacional plantea serias dificultades para la tutela de los datos y metadatos personales, que forman parte de los flujos transfronterizos característicos de las telecomunicaciones convergentes.
- Frente a esta realidad, actualmente es posible identificar potenciales soluciones en las propuestas de coordinación, interoperabilidad y cooperación internacional, el planteamiento de tratados internacionales sobre protección de datos personales y la implementación de las más diversas soluciones técnicas.
- Si bien nuestra Ley Nº 8642 y su normativa conexa brindan un nivel de protección aceptable a la privacidad de los usuarios finales de los servicios de telecomunicaciones en el ámbito nacional, esta normativa no extiende dicha protección a los servicios de información.
- Dadas las limitaciones encontradas en la Ley Nº 8968, la difícil situación de PRODHAB y la limitada gama de convenios internacionales vinculantes, resulta imposible afirmar que Costa Rica garantice adecuadamente la protección de datos personales en las telecomunicaciones convergentes.

# Ficha Bibliográfica

Quesada Rodríguez, Adrián. Protección de datos en la convergencia de las telecomunicaciones: el caso de Costa Rica. Tesis de Licenciatura en Derecho, Facultad de Derecho. Universidad de Costa Rica. San José, Costa Rica 2014. xx, 840.

Director: Prof. Dr. Eric Alfredo Chirino Sánchez

Palabras clave: telecomunicaciones convergentes, protección de datos personales, personalidad virtual, derecho a la intimidad, derecho a la privacidad, derecho a la información, derecho a la autodeterminación informativa, seguridad de la información, sociedad de la información y la comunicación, tecnologías de la información y la comunicación, Internet, bases de datos, datos sensibles, datos de tráfico y localización, metadatos, transferencias internacionales de datos personales.

# Introducción General

> "Siempre los ojos que os contemplaban y la voz que os envolvía. Despiertos o dormidos, trabajando o comiendo, en la casa o en la calle, en el baño o en la cama, no había escape. Nada era del individuo a no ser unos cuantos centímetros cúbicos dentro de su cráneo".
> George Orwell, 1984

Sesenta y cinco años después de la publicación de 1984, las prevenciones realizadas por Orwell han dejado ya de pertenecer a un futuro distópico y se nos presentan hoy como parte indiscutible de nuestra realidad. Las tecnologías de la información y la comunicación rodean y controlan todos los aspectos de nuestras vidas. Vivimos en un mundo que requiere nuestra conexión constante y absoluta a las redes de información y castiga, con extrañamiento y suspicacia, a todo aquel que rehúse ser parte de esta nueva comunión tecnológica.

La tecnología ha permitido al mundo entero conocer aún los más exiguos aspectos de un individuo. Nuestras ideas, intereses, movimientos y deseos son ahora meros datos por ser recopilados, cuantificados y clasificados en su paso por las redes de información; y esta realidad, aceptada por todos como una consecuencia inevitable de nuestra vida en sociedad, hoy nos torna en verdaderos *hombres de cristal*.

En un mundo marcado por el constante intercambio de unos y ceros, la información personal es vista como un bien disponible. Por ello, los individuos a quienes esta información hace referencia han dejado paulatinamente de ser considerados usuarios,

para convertirse en los productos que valorizan los sistemas estatales y corporativos de información.

Inadecuadamente protegido por las instituciones sociales, las leyes y los preceptos formulados por sus predecesores, el individuo se ve forzado a ceder sus intereses ante la imposible realidad con la que se enfrenta. Al hacerlo, incentiva la adopción de prácticas aún más invasivas y esto da lugar a un círculo vicioso del cual le resulta imposible escapar.

*"Sin respeto a la vida privada, la libertad es una quimera"* (Morales Godo, 2009, págs. 161-163). Esta es la realidad de incontables ciudadanos del mundo que, víctimas de la globalización descontrolada, ven afectados actualmente sus derechos por Estados y corporaciones; quedan sin más opción que aceptar al irrespeto de su intimidad, so pena de ser exiliados por la brecha digital y ser tachados como "*"alguien que tiene algo que esconder", y, automáticamente, en sospechoso, en "enemigo del pueblo"* " (Rodotà, 2005).

Frente a tan pernicioso panorama, no podemos más que recordar a John Diebold y plantear junto a él la siguiente interrogante: *"Cuando se disponga de medios para elaborar un registro de todos nuestros actos, y se tenga acceso a ese registro, ¿quién será capaz de autolimitarse en su uso y abuso? A medida que vayamos logrando el poder de control del comportamiento humano, ¿quién decidirá cómo utilizarlo?" (Diebold, 1974, pág. 34).*

Este es el problema fundamental que rodea a la protección de datos en la actualidad, la cual procura encontrar un necesario punto de equilibrio entre la tutela de la autodeterminación informativa del ser humano, a la vez que permite el libre tránsito de la información que nuestra sociedad tanto requiere.

Si el conflicto entre el derecho a la vida privada y la libertad de información cobra singulares características con el desarrollo de la informática, su reciente masificación por medio de las tecnologías de telecomunicaciones convergentes lo eleva a proporciones nunca antes imaginadas. La capacidad de brindar múltiples servicios por medios móviles y de bajo precio ha extendido exponencialmente la cantidad, calidad y clase de información personal a la que tienen acceso estos sistemas.

La reciente apertura de los mercados de telecomunicaciones en Costa Rica ha implicado un cambio radical en la manera en que los habitantes de nuestro país se comunican y acceden a la información. En este contexto, examinar la situación actual de las técnicas y herramientas disponibles para la defensa de los datos personales de los usuarios de telecomunicaciones convergentes adquiere una relevancia indiscutible para nuestro país.

# Problema e Hipótesis

## Problema

Pese a encontrarse inmerso en los procesos de cambio de paradigmas generados por la convergencia de las telecomunicaciones, nuestro país no logra proteger de manera efectiva el derecho de los usuarios a la protección de sus datos personales en un contexto global.

## Hipótesis

1) La dependencia de los sistemas de telecomunicaciones convergentes en el intercambio a gran escala de información, aunada con la inexistencia de un consenso internacional sobre qué datos pueden ser tratados, retenidos y transmitidos, implica para los usuarios un constante estado de vulnerabilidad ante entes públicos y privados, quienes se encuentran interesados por igual en obtener y tratar sus informaciones sensibles.

2) El que nuestro país no se encuentre adscrito a un sistema internacional dirigido a la protección de datos personales, representa un límite a la capacidad del usuario costarricense de tecnologías convergentes de telecomunicaciones para salvaguardar sus derechos de privacidad y autodeterminación informativa más allá de los límites jurisdiccionales de su país.

3) El sistema actualmente implementado por el marco normativo nacional se encuentra limitado para defender los derechos de sus ciudadanos ante los retos planteados por la convergencia de las telecomunicaciones y la globalización de los servicios de información. Pese ser relativamente novedosa, la normativa costarricense no solo presenta errores y omisiones, sino que no logra alcanzar las tendencias y estándares implementados por los principales modelos regulatorios internacionales en materia de protección de datos.

# Objetivo General y Objetivos Específicos

## Objetivo General

1. Analizar con profundidad la implicancia de la protección de datos personales en el ámbito de los servicios de información y de telecomunicaciones, de tal manera que se comprendan las ramificaciones y efectos derivados de la convergencia tecnológica y se genere una realimentación a partir del estudio de los modelos técnicos y regulatorios que tutelan los datos personales en el ámbito nacional e internacional.

## Objetivos Específicos

1. Realizar un estudio de los fundamentos históricos y teóricos de la protección de los derechos a la intimidad, privacidad, información y autodeterminación informativa desde el punto de vista de los derechos humanos, los derechos fundamentales, los derechos de la personalidad y el derecho internacional.

2. Identificar las bases teóricas e históricas de la protección iusinformática de los datos personales de cara a la convergencia de las telecomunicaciones, procurando para ello analizar los elementos funcionales, manifestaciones y problemática que caracterizan a esta tendencia tecnológica.

3. Compilar un listado de la principal legislación positiva que regula la protección de datos personales en el ámbito internacional, dando especial relevancia a las soluciones implementadas por grupos representativos de países o regiones, frente a los problemas relacionados con la convergencia de las telecomunicaciones y la transmisión, tratamiento y retención de datos personales.

4. Presentar el marco administrativo y legal que da sustento a las telecomunicaciones y la protección de datos personales en Costa Rica.

5. Realizar un análisis del estado actual de la protección de datos personales en Costa Rica frente a la convergencia de las telecomunicaciones, que permita advertir sus principales falencias a partir de los fundamentos teóricos y los casos de derecho comparado estudiados.

6. Plantear algunas recomendaciones dirigidas a adecuar el sistema nacional de protección de datos a las más altas tendencias y estándares internacionales.

## Metodología

A lo largo de la investigación se utilizará un modelo híbrido de metodología, la cual se basará en un estudio esencialmente exploratorio de la regulación internacional y nacional sobre telecomunicaciones y protección de datos personales, dejando abierta la posibilidad de utilizar elementos descriptivos, correlacionales y explicativos sobre estos y otros temas relacionados.

Para la comprobación de las presentes hipótesis se aplicará fundamentalmente el método documental deductivo, partiendo de aspectos generales tales como los aspectos teóricos e históricos de las telecomunicaciones y el derecho a la protección de datos, hasta llegar a la regulación y aplicación de tal derecho en los aspectos específicos a la transmisión, tratamiento y retención de datos en los sistemas de telecomunicaciones convergentes en la actualidad costarricense.

Asimismo, se utilizará el método comparativo con miras a determinar las soluciones encontradas por diversas legislaciones e instituciones internacionales, mediante la lectura de material doctrinario, jurisprudencial y normativo. Esto con miras a realizar comparaciones fundadas y encontrar soluciones aplicables al plano nacional.

Con base en lo anterior, no se excluye la posibilidad de incorporar fuentes empíricas. Ello lo irá sugiriendo el mismo desarrollo de la investigación y la sensibilidad del investigador.

# Título Primero: Marco teórico de la protección de datos

## Capítulo I: Intimidad, Privacidad, Información y Autodeterminación Informativa como Derechos Humanos

A lo largo del presente capítulo se expondrán los fundamentos de los derechos a la intimidad, privacidad, información y autodeterminación informativa. Para ello, se dará inicio mediante un estudio de la historia que rodea el reconocimiento de la personalidad y dignidad humana, como fundamentos de la protección legal que legitima los derechos individuales y la evolución de los conceptos que los han enmarcado.

A continuación se estudiarán las diferencias existentes entre los *derechos humanos, los derechos fundamentales y los derechos de la personalidad* con miras a definir claramente el carácter de los derechos en cuestión; finalmente, se examinarán con más detalle las características elementales de estos cuatro derechos humanos, mencionando brevemente el marco legal nacional e internacional que los rodea.

## Sección I: Fundamentos Teórico-Históricos de la Protección de la Personalidad por los Derechos Humanos

La presente sección iniciará realizando un estudio de la evolución histórica de la protección de los derechos de la personalidad humana y el surgimiento del concepto de "derechos humanos". Dicha travesía conducirá desde dos de las más influyentes civilizaciones de la antigüedad (Grecia y Roma), hasta culminar con el desarrollo de los derechos humanos y el surgimiento de nuevas manifestaciones legítimas de la personalidad humana frente a los grandes desarrollos tecnológicos del último siglo.

Una vez comprendido los fundamentos históricos de la protección de la personalidad y la dignidad humana, se enfocará la atención en la determinación de los fundamentos teóricos de los derechos que rodean a la protección de datos personales en la actualidad.

Para tal fin, se detallarán los conceptos de derechos humanos, derechos fundamentales y derechos de la personalidad en sus múltiples definiciones, fundamentos, características y (en caso de encontrarse) clasificaciones, buscando de esta manera esclarecer su relación con los derechos a la intimidad, la privacidad, la información y la autodeterminación informativa.

## *Breve Introducción Histórica*

Los derechos humanos son el resultado de la evolución histórica del rol del individuo respecto al poder. Son parte de una construcción legal que, en comparación con la historia de nuestra especie humana, es sumamente reciente y que ha culminado con la reconceptualización de la persona y el reconocimiento de su plena personalidad, como sujeto de derechos y obligaciones, tanto con respecto a otros individuos como respecto al Estado.

Esta evolución histórica, marcada por la concentración del poder en grupos pequeños de individuos y las diversas revoluciones que han llevado a cambios en la distribución de tal poder, ha permitido la superación del *estado de naturaleza*[1] y la creación de un marco legal estable que regule y garantice, aún en el plano internacional, el conjunto de prerrogativas inalienables e inherentes a todos los miembros de la familia humana, que permiten al individuo el desarrollo holístico de su personalidad.

Con miras a lograr los objetivos del presente capítulo, a continuación se examinarán los procesos históricos que llevaron al reconocimiento de la dignidad humana, la privacidad, la intimidad, la información y la autodeterminación informativa como derechos humanos.

[1] Caracterizado por Tomás Hobbes por imperar en él la lucha del hombre contra el hombre y la inexistencia de leyes que regulen las relaciones entre los seres humanos.

## Antigüedad

En los inicios de la historia de la humanidad, *"no es posible hablar de derechos del hombre como conjunto de prerrogativas del gobernado de observancia jurídica obligatoria e imperativa para los gobernantes" (Burgoa Orihuela, 1996, pág. 58)* esto debido a que el concepto mismo de persona poco tenía en común con aquel que actualmente sostenemos.

La inexistencia de prueba documental sobre las costumbres imperantes en la prehistoria implica, para los fines de esta investigación, la necesidad de suponer que los pueblos de entonces se guiaban por sistemas matriarcales o patriarcales en los que resultaba desconocido cualquier concepto de derechos individuales como *"conjunto de prerrogativas del gobernado de observancia jurídica obligatoria e imperativa para los gobernantes"* (Zamora Hernández, 2007) y en los cuales la ley del más fuerte era de aplicación ordinaria.

Aun avanzando en la historia hacia pueblos antiguos tales como Mesopotamia, Egipto, Asiria, Palestina o Persia, sobre los cuales existen pruebas fehacientes de su historia y modelos de vida, es posible observar la inexistencia del concepto de derechos humanos y el *"completo desconocimiento de cualquier concepto de derechos individuales"* dada la existencia de *"soberanos fundamentados sobre el poder divino y con poder absoluto sobre sus pueblos"* (Lions, 1969).

Según Monique Lions, en la antigüedad la omnipotencia del soberano era fundamento suficiente para la eliminación total de la personalidad jurídica del individuo, el cual era visto simplemente como una fuente de mano de obra, cuyo único valor como material

humano residía en su utilización para realizar aquellas obras que por motivo de política, religión, subsistencia o guerra resultaran más provechosas para el soberano.

Aún con el posterior surgimiento de las llamadas *Tablas de la Ley* alrededor de 590 a.C. (Lions, 1969, pág. 480), las cuales establecían disposiciones tanto civiles, como religiosas y penales, es posible afirmar que estas no establecían limitación alguna al poder absoluto del monarca sobre sus súbditos, lo cual se ve reafirmado por el conocido destino de los prisioneros de guerra, tanto civiles como combatientes, durante esta época.

Tal vez la única excepción que podría encontrarse a tal situación se encuentra en la sociedad China, en la cual desde 800 hasta 200 a.C., "*filósofos como Confucio y Lao-Tsé predican igualdad entre los hombres, argumentan democracia como forma idónea del gobierno, así como derecho legítimo del gobernado para revelarse contra los tratos déspotas y arbitrarios"* (Barreiro, 1981, pág. 10).

Desde el punto de vista de la protección a la intimidad en la época antigua, autores como Ruiz Miguel, Maclver y Westing han puesto en evidencia que *"la protección de la intimidad en los pueblos primitivos es menor, o cuando menos distinta de la que es usual en nuestros días"* (Ruiz Miguel, 1997, pág. 11) y demuestran, a lo largo de sus estudios que tanto en Oriente como en Occidente, la vida en la antigüedad se caracterizaba por una sumisión del individuo a los usos y costumbres imperantes en su pueblo, en la cual existía tan solo una manera correcta de hacer las cosas, la cual era dictada por la teocracia (nuevamente, identificada con la deificación del gobernante o por designio de una casta sacerdotal).

Tal situación implicaba la inexistencia práctica en la antigüedad de un concepto similar al que actualmente manejamos en materia de intimidad. El peso de las costumbres y comportamientos fijados tenía como consecuencia para el individuo la subordinación a lo público, aún de las cuestiones más privadas de la vida humana. Ejemplo de lo cual nos brinda, Constant al afirmar que, por ejemplo en Egipto antiguo, *"todo estaba regulado por la ley, hasta las distracciones, hasta la necesidad, cada momento del día e incluso el amor"* (Ruiz Miguel, 1997, pág. 12).

## Grecia Clásica

En la historia occidental, es a partir de la Grecia Clásica donde tradicionalmente se identifica el punto de inicio de las corrientes filosóficas tendientes a dignificar la concepción del ser humano. Así, durante esta época surgen las primeras ideas humanistas basadas en la percepción del Derecho como normas morales y jurídicas, universalmente válidas y asequibles a la razón humana (iusnaturalismo).

Asimismo se encuentra durante esta época el surgimiento de la tendiente filosófica del Estoicismo, la cual *"surge en cultura occidental como una idea dignificadora del hombre, entendiendo que todo el género humano está hermandado por la razón y con ellos surge también la idea de la ley natural, al concebir que el orden de la naturaleza es eterno e inmutable, por ello el proceso de lo natural en armonía con la razón, refleja el carácter divino del universo" (Zamora Hernández, 2007).*

Con base en estos fundamentos filosóficos inició en la sociedad helénica la creación de un revolucionario sistema político en el cual *"el elemento básico era el individuo libre. Esparta, Atenas, Tebas, conocieron esa diferenciación de clases sociales, característica de la antigüedad, que dividía la sociedad en hombres libres y en esclavos, con todos los matices que afectaban esa distinción: ilotas, artesanos, marineros, sirvientes, no desempeñaban papel alguno en la vida de la polis, ni en el terreno civil ni en el político"* (Lions, 1969).

Conocido como *democracia aristocrática* este sistema constituyó el primer ejemplo de participación popular en el gobierno de la ciudad, pues se caracterizaba por delegar las funciones políticas en unos pocos ciudadanos, vistos por la sociedad como los mejores. Este sistema aristocrático fue posteriormente sustituido por un sistema de democracia directa, instituido por políticos como Solón, Clístenes y Elfialtes de Atenas, quienes poco a poco lograron su institución como un sistema político caracterizado por brindar el poder político a los ciudadanos, quienes lo ejercían mediante la participación ciudadana directa con independencia de su capacidad económica.

En este contexto, los aportes realizados por la sociedad helénica a la dignificación de la persona humana[2] resultan indudables, y a pesar de la existencia de marcadas clases sociales que excluían aún a gran parte de la población de la ciudad, los múltiples avances políticos y filosóficos generados durante esta época marcaron profundamente el desarrollo de la historia mundial.

Ahora bien, con respecto al concepto y protección de la intimidad individual, Ruiz Miguel nos recuerda que *"un rasgo característico de la idea de Estado de los griegos (…) es el*

[2] En palabras de Lions, la Grecia Antigua reconoció de manera clara *"la eminente dignidad de la persona humana con el concepto de esas "leyes no-escritas" que ya obligaban a la Antígona de Sófocles…"* (Lions, 1969, pág. 481).

*valor ilimitado que se atribuye a la comunidad, valor de tal magnitud que la existencia de una esfera reservada a la vida propiamente personal del ser humano estaba, en principio, excluida" (Ruiz Miguel, 1997).*

Tal característica es, en el pueblo helénico, resquicio quizá de la época antigua; sin embargo, se diferencia de esta en tanto en Grecia la participación en comunidad y en la organización estatal es vista como necesaria dada la íntima relación entre todas las actividades humanas con las estatales, en una sociedad que imaginaba al hombre como *"un ser primordialmente social y no individual"*. En palabras de Constant *"El individuo, soberano casi siempre en los asuntos públicos, era un esclavo en todas las cuestiones privadas" (Ruiz Miguel, 1997, pág. 12).*

### Roma

En la sociedad romana, la concepción de personalidad comparte la división característica de las sociedades antiguas, consistente en el completo reconocimiento de derechos para cierto grupo de ciudadanos, a la vez que se negaba la personalidad de los demás miembros de la sociedad. A pesar de ello, el Derecho romano contaba con una mayor flexibilidad y adaptabilidad con respecto al vigente en la sociedad de la Grecia Antigua, y es precisamente tal característica la que le permitió convertirse en referente del Derecho actual.

En la sociedad Romana el *pater familias* era considerado *"único portador de los status de familia, libertad y ciudadanía"* (Costa, 2008, pág. 6); era el único individuo reconocido como

sujeto de derechos ante el Estado[3], *"los cuales ejerce libremente y que son sancionados judicialmente conforme al Jus civile quiritium de la época monárquica (753 a. C. – 509 a. C.)" (Lions, 1969, pág. 481),* mientras que ni sus esclavos ni los demás miembros de la familia eran reconocidos como individuos siquiera.

Tal situación se mantuvo aún tras la promulgación de la Ley de las XII tablas (451 a. C.), en la que, si bien se produce el reconocimiento de la autonomía individual, el derecho de defensa de la libertad personal y fueron establecidas algunas sanciones ante crímenes contra el honor y la fama del individuo libre (De la Parra Trujillo, 2001, pág. 142), el Derecho romano continuaba considerando como sujeto de derecho únicamente al pater familias, al cual se reconocían derechos absolutos sobre los miembros de su familia[4].

A pesar de lo anterior, debido a transformaciones profundas dadas durante el Imperio, esta tendencia comenzó a retrotraerse y ya para 212 d. C. fue otorgado el estatus de ciudadanos a todos los individuos libres. Aunado a tal situación, para finales del Imperio, los derechos absolutos del pater familias para con su familia comenzaron a menguar *(Lions, 1969, pág. 182)*.

Desde el punto de vista filosófico, es en la Roma Imperial donde se puede identificar una verdadera evolución del Derecho natural (uno de los fundamentos originales de los derechos humanos). El iusnaturalismo encuentra acogida en el pensamiento de

[3] Según historiadores como Lowënstein, el sistema romano garantizaba, aún para los ciudadanos, solamente derechos políticos, y no existía en el derecho romano el equivalente a los derechos fundamentales y colectivos actuales dado que los romanos mismos no concebían derecho alguno contra el Estado *(Ruiz Miguel, 1997, pág. 19) (Zamora Hernández, 2007, pág. 2)*.
[4] La cual era vista como un *"cuerpo único compuesto de bienes y personas"* sobre el cual éste podía hacer todo lo que deseara (Costa, 2008).

Cicerón[5] y sus fundamentos son posteriormente adoptados dentro de la concepción estoica de Gayo, quien distinguiera entre el *Ius Civile*[6] y el *Ius Gentium*, el cual era considerado por el autor como un derecho revelado por la razón y común a todos los pueblos.

Por otra parte, en materia de protección a la intimidad, Ruiz Miguel señala que la doctrina suele asimilar la situación de Roma con la de Grecia y apunta tres ejemplos de leyes que señalan hacia un *"desconocimiento de la intimidad"* citadas por Montesquieu en sus obras como historiador del Derecho[7], a partir de lo que el autor concluye que *"los romanos ignoraban la intimidad como principio rector de su legislación subordinando a la persona a lo público hasta extremos que hoy juzgamos intolerables"* (Ruiz Miguel, 1997, pág. 21).

A pesar de lo anterior, hacia el final del Imperio romano, conforme el catolicismo adquiere cada vez mayor influencia en la sociedad romana, la libertad de religión de los ciudadanos romanos es reconocida mediante el Edicto de Milán[8] del año 313. Tal hito puede ser visto como un precedente importante al reconocimiento de la intimidad individual, al constituir el primer ejemplo de una efectiva limitación estatal frente a un aspecto de la intimidad individual.

[5] Quien alrededor del año 53 a. C. ya consideraba que el Derecho se encontraba fundamentado en la naturaleza humana y no en la voluntad humana y afirmaba que "*En cualquier materia el consenso de todos los pueblos ha de considerarse ley de la naturaleza*".
[6] Derecho tradicional romano aplicable solamente a los ciudadanos.
[7] A saber: el carácter públicamente acusable del adulterio; el juramento que cierto Corvilio debió brindar ante los Censores ante la esterilidad de su mujer dirigido hacia repudiarla con tal de dar hijos a la república y la prohibición establecida por la ley de "matrimonios inútiles" con tal de promover la natalidad.
[8] En el cual se establecen los fundamentos de la libertad de religión al establecerse una "neutralidad religiosa efectiva" por parte del imperio frente a los súbditos.

Esta aceptación del catolicismo dentro del Imperio terminó por calar en los teóricos de la época, quienes poco a poco adquirieron consciencia sobre la importancia de la intimidad. En este contexto, San Agustín[9] debe ser reconocido como el primer teórico en abarcar de manera profunda el tema de la intimidad y es esta la idea central de un considerable número de sus obras.

## Edad Media

La Edad Media, dividida tradicionalmente en dos (Alta y Baja) por los historiadores, significó un cambio radical en la evolución del derecho en Occidente. La caída del Imperio romano y la posterior creación de regímenes feudales a lo largo de Europa, implicó la *"ruptura del principio de omnipotencia del Estado" (Lions, 1969, pág. 482)* a favor de un sistema basado en vínculos personales entre el señor feudal y sus siervos.

Según Lions, la feudalidad implicó en la Edad Media la confusión entre propiedad y soberanía por parte del señor feudal. Esta situación se traducía en el reconocimiento pleno de la personalidad del señor mientras que al siervo le era reconocida una personalidad limitada a su esfera doméstica.

Esta situación tuvo como consecuencia para el hombre *semi-libre* una servidumbre que *"traducía una dependencia que no era absoluta. Al contrario del esclavo romano, el siervo de la Edad Media tenía una personalidad: podía poseer bienes muebles y ejercía tanto la patria*

[9] Según Ruiz Miguel, San Agustín desarrolla su teoría del conocimiento a lo largo de su obra *Las Confesiones*, en la cual el autor "identifica conocimiento y Dios" (Ruiz Miguel, 1997, pág. 27) e invita a la exploración de la intimidad, tratando esta y varios de sus elementos en el mismo sentido que el utilizado en la actualidad.

*potestad como la marital. Pero este estado de siervo constaba de incapacidades de derecho público y de obligaciones múltiples (…) Por otra parte, la persona física del siervo pertenecía al señor, quien, además gozaba de varias prerrogativas sobre el patrimonio servil"* (Lions, 1969, pág. 482).

A pesar de la existencia extendida de relaciones de servidumbre marcadas por limitaciones a los derechos individuales, no toda la Edad Media puede ser caracterizada por esta prepotente autoridad del señor feudal sobre sus siervos.

Uno de los puntos más relevantes de la época tuvo lugar durante la Alta Edad Media cuando en el año de 1215, el rey Juan I de Inglaterra (mejor conocido como Juan sin Tierra) aceptó firmar la llamada *Carta magna de las libertades*. Este documento es considerado en la actualidad como uno de los principales precursores a las declaraciones de derechos modernas, en tanto en él fueron establecidos por vez primera límites al poder del Estado frente a sus súbditos (Torres, 2002).

La Edad Media también supuso una época de fuertes polémicas filosóficas entre los pensadores de la época, quienes se debatían con respecto al reconocimiento de la existencia de derechos naturales. Es en este contexto que surge la concepción eclesiástica del Derecho natural[10]. Representada fundamentalmente por la *Patrística* de San Agustín y la *Escolástica* de Santo Tomas de Aquino[11], esta concepción adquirió finalmente una gran aceptación durante la época, lo cual facilitó en el largo plazo, la aceptación de la existencia de derechos comunes a todos los individuos.

[10] La cual establece básicamente que el Derecho no puede oponerse a las revelaciones divinas.
[11] Las cuales desarrollan el llamado *iusnaturalismo teológico*, basado en la noción de dignidad humana universal fundamentada en la voluntad divina.

Finalmente debe recalcarse que gracias al gran ímpetu del cristianismo durante la Edad Media, el reconocimiento de la libertad individual fue también objeto de grandes discusiones filosóficas pues *"el Cristianismo planteó un problema que no había conocido el mundo antiguo, el problema de las relaciones entre Iglesia y Estado, y supuso una diversidad de lealtades y un JUICIO INTIMO no incluido en la idea de ciudadanía" (Ruiz Miguel, 1997).*

## Del Renacimiento hasta el Siglo XVII

El Renacimiento significó para el Derecho la superación de la hegemonía eclesiástica característica de la Edad Media, a partir de la corriente laicista iniciada por los escritos de Dante, Bocaccio y Petrarca. Asimismo, el Renacimiento representó la restauración del concepto del derecho absoluto del Estado, en el cual el poder legislativo radicaba en el rey.

Al respecto, señala Ruiz Miguel que Toynbee observa cómo durante esta época *"se produjo un Renacimiento de ciertas ideas e instituciones políticas de la antigüedad helénica, como la del estado-ciudad (que) prepararon el terreno para que surgiese la figura, también helénica, del tirano" (Ruiz Miguel, 1997).*

Precisamente es dentro de este marco que se encuentran las obras de Maquiavelo, quien otorga el papel de organizador y rector de una sociedad corrupta al legislador, aun cuando esto signifique un *"perjuicio al reconocimiento de la dignidad de las personas y supone una menor atención a la intimidad"* (Ruiz Miguel, 1997).

Ya en el Siglo XV, el conde Giovanni Picco della Mirandola escribe sobre la dignidad del hombre en su *De hominis dignitate* (*Oración sobre la Dignidad del Hombre),* obra que se constituyó en un verdadero *manifiesto del renacimiento* al intentar llamar la atención sobre la perspectiva y capacidad humana. A lo largo de este texto, el autor exalta el potencial humano a la vez que hace énfasis en la importancia de la búsqueda humana del conocimiento, la dignidad de las artes liberales y la filosofía.

El Siglo XVI encontró en autores como Rinuccini, Giordano Bruno y Tomás Moro, sus principales avances hacia la concepción de la dignidad humana. Así, los trabajos del arzobispo Giovanni Battista Rinuccini desarrollan los temas fundamentales de la libertad humana. Giordano Bruno, caracterizado como un *mártir de la ciencia* por autores como A. M. Paterson, se refiere a la dignidad y la liberación del hombre del temor a la muerte y a los dioses buscando mejorar la ciencia y el conocimiento de las cosas naturales. Por su parte, Tomás Moro, abogado y filósofo social inglés acuñó el término *Utopía* con su obra del mismo nombre, la cual trata sobre la dignidad humana y el significado de la nobleza.

En el Siglo XVII, autores como Johannes Althusius y Tomaso Campanella tratan temas relacionados con el desarrollo de la ciencia y la dignidad humana. Asimismo es en este siglo que Baltasar Gómez de Amescúa publica su libro "*Tractus de potestate in se ipsum"*, el cual es seguido, años después, por la publicación por Samuel Stryck de su obra "*De iure hominis in se ipsum"*.

A lo largo de sus obras, tanto Gómez de Amescúa como Strick exponen la teoría del "*ius in se ipsum"* o (derecho sobre sí mismo), también llamada *"potestas in se ipsum o ius*

*in corpus"* (De la Parra Trujillo, 2001, pág. 142), la cual se constituye en fundamento de la actual teoría de los derechos de la personalidad.

Los desarrollos doctrinales del Siglo XVII conllevan el tratamiento del racionalismo y el iusnaturalismo por parte de autores como Hugo Grocio y Francisco Suárez, quienes junto con los demás integrantes de la Escuela del Derecho Natural, hicieron posible la construcción de *"la teoría de los derechos naturales o innatos que finalmente deriva en doctrina de matiz político y revolucionario: la de los derechos del hombre y del ciudadano"* (De la Parra Trujillo, 2001, pág. 143).

### Siglo XVIII

De suma importancia para los derechos humanos y la defensa de la intimidad, el Siglo XVIII vio en la Ilustración y la Declaración de Derechos del Hombre y el Ciudadano, el máximo apogeo del iusnaturalismo, el cual dio origen al concepto contemporáneo de derechos del hombre y a las revoluciones liberales que dirigieron la historia de los siglos posteriores.

Según Ruiz Miguel, la Ilustración *"atribuye a la información y a la libre expresión la función de crear una opinión pública capaz de discutir los problemas de gobierno" (Ruiz Miguel, 1997, pág. 50)* tras la que subyace la idea de libre discusión, la cual acarrea en su seno la transparencia informativa.

Los pensadores de la Ilustración sostenían básicamente que mediante la razón humana sería posible combatir la ignorancia, la superstición y la tiranía, con miras a la

construcción de un mundo mejor para las clases oprimidas por los estados totalitarios vigentes desde el Renacimiento.

En este contexto, la libertad de prensa se constituyó a la vez en herramienta y arma contra el secretismo característico de los Estados absolutistas, a la vez que contribuía a la popularización del conocimiento de la técnica (el cual históricamente había sido resguardado como bien casi sacrosanto por los gremios).

Desde esta perspectiva, los pensadores de la Ilustración buscaron la manera de recopilar la totalidad del conocimiento científico como medio para la eliminación del oscurantismo de las autoridades políticas y religiosas. La Enciclopedia se constituyó así en una de las manifestaciones más importantes de la Ilustración, al ser esta una obra colectiva de grandes dimensiones, dedicada, en palabras de D'Alembert, a explicar *"discutir, analizar y agitar todo (…) desde las cuestiones que más nos atraen, a las que nos interesan más débilmente"* desde un punto de vista laico.

Al respecto del afán a favor de la libertad de información existente en la Ilustración, Ruiz Miguel recuerda que *"un funcionamiento ortodoxo de este sistema exige plena transparencia informativa, y por tanto, resulta virtualmente vulnerador de toda intimidad que oculte cualquier circunstancia que resulte de interés para quienes estén en el poder, sea el Parlamento o sea un periódico" (Ruiz Miguel, 1997, pág. 51)*, por lo que el desarrollo de tal libertad termina por plantearse siempre la necesidad de fijar sus límites.

Las ideas sostenidas a largo de la Ilustración se ven reforzadas en 1776 por la Declaración de Independencia de los Estados Unidos de América, documento fundamental del movimiento independentista estadounidense en el cual se establecen

desde sus inicios algunos derechos fundamentales del individuo basados en el iusnaturalismo al proclamar *"como verdaderas evidencias que todos los hombres nacen iguales, que están dotados por su creador de ciertos derechos inalienables, entre los cuales se encuentra el derecho a la vida, a la libertad y a la búsqueda de la felicidad..." (Torres, 2002).*

La Ilustración culmina cuando, en 1789 da inicio la Revolución francesa, fundamentada alrededor de las ideas de Montesquieu, Rousseau y Voltaire, en las cuales resulta evidente la influencia iusnaturalista, desde la perspectiva del hombre como titular de derechos naturales inalienables e intransferibles permanentemente a gobernante alguno *(Lions, 1969).*

Precisamente la Revolución francesa intenta solucionar el problema político que supone conciliar la libertad del hombre con la necesidad de vida en un Estado, problema que, desde la perspectiva del pueblo, el Estado absolutista había fracasado en solucionar.

Esta búsqueda, por parte del pueblo francés, de un régimen político ideal que consagre y proteja los derechos y la dignidad humana, culmina cuando en 1789, la Asamblea Nacional Constituyente francesa aprueba la Declaración de Derechos del Hombre y el Ciudadano *(Lions, 1969)*.

Esta Declaración se constituye hoy como punto de referencia en materia de derechos humanos individuales, al ejemplificar la máxima riqueza del desarrollo conceptual de su época sobre los derechos del individuo frente al Estado *(Torres, 2002, pág. 5),* cuyo contenido fue adoptado por gran parte de los movimientos constitucionalistas que tuvieron lugar en el ámbito mundial a partir de la fecha.

La Declaración de Derechos del Hombre y el Ciudadano tiene, para el área de la intimidad individual, una particularidad que Ruiz Miguel señala acertadamente: la Declaración no recoge dentro de su texto ninguna de las manifestaciones de la intimidad (Ruiz Miguel, 1997, pág. 51).

### Siglo XIX hasta Siglo XX

La historia de los siglos XIX y XX es fundamental para la evolución de los derechos humanos, en tanto es en ella donde se producen los eventos que llevan a su configuración actual.

A pesar del ímpetu obtenido a lo largo de la Ilustración y la Revolución francesa, el Siglo XIX se encontró marcado tanto por el pensamiento individualista y liberal como por el declive del iusnaturalismo. Tal declive fue causado fundamentalmente por el surgimiento de dos nuevas teorías que intentan realizar una relectura del Derecho y buscar su propia justificación de los derechos del hombre, superando el iusnaturalismo.

La primera de estas dos teorías, el *historicismo jurídico*, es sostenida por la escuela histórica del Derecho; surge como un movimiento que reacciona contra el ímpetu racional que caracterizó a la Ilustración e intenta encuadrar al Derecho como producto colectivo e inconsciente del contexto histórico de la humanidad. Esta escuela histórica, de la cual forman parte autores como Gustavo Hugo y Federico Carlos Savigni, exalta el sentimiento sobre el entendimiento y adopta una postura romántica que no admite la

noción de un ente centralizado capaz de establecer leyes generales, sino que da preferencia a la creación casuística de normas acordes con su contexto.

Una segunda teoría, el *positivismo jurídico*, busca exaltar el rol del Estado como productor del Derecho y caracterizar a todo Derecho propio de un Estado determinado. Esta teoría responde al entusiasmo producido a partir del Código de Napoleón, el cual comprenden como obra de hombres, no de pueblos o de la historia y como una producción racional que se convierte, por voluntad del Estado, en Derecho estatal (Antillón Montealegre, 2013).

La corriente constitucionalista que da inicio con la declaración de independencia de los Estados Unidos de América y la Revolución francesa, aunada con el éxito de la ideología liberal, resultan finalmente en la adopción por parte de la mayoría de los Estados modernos, de sistemas de Derecho basados en el positivismo jurídico. Es gracias a tales justificaciones teóricas que durante el Siglo XIX surge la adopción de las primeras normativas que, en el ámbito mundial contemplan los derechos inherentes de las personas, tales como el Código Civil de Austria de 1811 y el Código Civil Portugués de 1867 (Lions, 1969).

A pesar de lo anterior, se debe resaltar que el siglo XIX se encontró marcado fundamentalmente por la inequidad social causada por el capitalismo que caracterizó la Revolución Industrial, la cual da inicio en Gran Bretaña y se expande por la mayor parte de la Europa Continental a lo largo de la segunda mitad del siglo.

La Revolución Industrial tuvo consecuencias para la calidad de vida del individuo promedio, las cuales se extendieron incluso a su intimidad. Sobre este punto, Ruiz

Miguel escribe que *"Sobre todo al principio de la Revolución Industrial, se manifestó crudamente la virtualidad "anti-íntima" de la urbanización, aunque con el tiempo desvaría en desencadenante de soledad-intimidad. El crecimiento de las ciudades en el período de la Revolución Industrial se hizo de forma rápida y sin ningún tipo de planificación lo que produjo unas condiciones de vida en los barrios ocupados por las clases trabajadoras muy penosas"* (Ruiz Miguel, 1997, pág. 56).

Las injusticias causadas por la Revolución Industrial, la economía capitalista y los procesos de urbanización desmedida de la época, se manifestaron en dos frentes especialmente relevantes para la presente investigación. Por un lado, *"tuvieron su traducción en la dimensión de la intimidad como idea" (Ruiz Miguel, 1997, pág. 72)* que mantenemos en la actualidad y, por otra parte, dieron pie en el siglo XX[12] a las reivindicaciones laborales que finalmente determinaron la consagración actual de los llamados derechos económicos y sociales *(Torres, 2002)*.

Asimismo, debe recordarse que ya hacia el final del siglo XIX, el desarrollo del concepto de "dignidad humana" fomentó también el crecimiento paralelo de teorías jurídicas que afirmaban la posesión, por parte de toda persona, de un derecho general a su propia personalidad.

Esta teoría, fundamento de los actuales derechos de la personalidad, fue reconocida inicialmente *"por la codificación suiza del derecho de obligaciones (Cód. Suizo, artículo 49), por la doctrina civil alemana (Zweigert/Kötz 1996 695) y por el derecho civil francés desde fines del siglo XIX (Tallon 1996 Nº 1)" (Morales Godo, Instituciones del Derecho Civil, 2009, pág. 535).*

[12] Específicamente con la Revolución Mexicana de 1910 y Rusa de 1917 (Torres, 2002).

Por su parte, el siglo XX se ve marcado desde la perspectiva de los derechos humanos, fundamentalmente por las dos guerras mundiales ocurridas a principios de este. Los efectos producidos por guerras de escala suficiente como para afectar al mundo entero, aunadas con las desgracias producidas durante el holocausto, impulsaron en un nivel global la búsqueda del establecimiento de mecanismos internacionales capaces de prevenir que tales hechos se repitieran y finalmente la adopción global de los derechos humanos tal como son concebidos en la actualidad.

A principios del Siglo XX, la noción aceptada de Derecho Internacional afirmaba que este derecho se preocupaba solamente por la regulación de las relaciones interestatales y negaba al particular todo derecho de participación en el ámbito internacional.

La Primera Guerra Mundial, conflicto bélico iniciado en 1914, involucró a todas las grandes potencias del mundo y tuvo como consecuencia el primer movimiento internacional para la reorganización de las relaciones internacionales por medio de la creación de la *Sociedad de las Naciones*.

La Sociedad de las Naciones fue un organismo internacional creado por medio del Tratado de Versalles el 29 de junio de 1919, basado en los principios de la cooperación internacional, el arbitraje de los conflictos y la seguridad colectiva. A pesar de presentar problemas evidentes en su estructura, evidenciados en su falta de autoridad para imponer sus resoluciones de forma obligatoria, la Sociedad de las Naciones es actualmente considerada como predecesora a la actual Organización de Naciones Unidas.

Ahora bien, a principios del siglo XX el mundo ve surgir también dos grandes corrientes del pensamiento que versan sobre el papel que debe jugar el individuo frente al Estado. La primera de estas corrientes, conocida como *"individualista"* establece que el *"Individuo es causa final de todas las instituciones sociales, y especialmente, del estado y del derecho" mientras que la segunda, conocida como "anti-individualista"* asegura que *"el individuo no es más que un medio, que no existe sino por y para una entidad, (Estado) que es un fin en sí mismo" (Lions, 1969)*.

En la Europa de la entreguerra (1918-1939) toma fuerza en Alemania e Italia esta corriente anti-individualista y se manifiesta en la realidad política y social de estos países por medio del fascismo. Según Lions, el fascismo puede ser caracterizado, en términos generales como una doctrina irracional que hace hincapié en la desigualdad natural de los hombres; es totalitario, comunitario y exalta la guerra *(Lions, 1969).*

En el caso italiano, el fascismo se manifiesta como un proyecto político no racista guiado por el "*Todo en el estado, nada contra del estado, nada fuera del estado"* (sic) *(Lions, 1969)*, en el cual el individuo desaparece ante la trascendencia y omnipotencia estatal. En el caso del *nacional-socialismo alemán (nazismo*), la ideología imperante lleva este proyecto político a sus extremos, caracterizándose por considerar que la *"Realidad primera es el Volk (comunidad racial)"*, que el *"El individuo no existe sino como miembro de la Volksgemeinschaft"* y que el *"Volk es entidad superior a seres, cuyo destino la deja perfectamente indiferente" (Lions, 1969)*.

Esta ideología lleva a Alemania a desencadenar la Segunda Guerra Mundial cuando, en 1939 invade Polonia (como un primer paso hacia su pretensión de fundar un gran imperio en Europa) y a llevar a cabo el Holocausto: el intento de aniquilar totalmente

la población judía de Europa. La Segunda Guerra Mundial (1939-1935) implicó la muerte de más de sesenta millones de personas, con lo que se configuró como el mayor conflicto bélico de la historia.

Tras la conclusión de la Segunda Guerra Mundial, cuarenta y seis Estados, entre los que se encontraban China, Francia, la Unión Soviética, el Reino Unido y los Estados Unidos de América, acuerdan la creación de una organización internacional dirigida a la prevención de la guerra, la cooperación, la paz y seguridad internacional, el desarrollo económico y social, los asuntos humanitarios y los derechos humanos.

Es de esta manera como, el 24 de octubre de 1945, es fundada la Organización de las Naciones Unidas con la entrada en vigor de la Carta de las Naciones Unidas, a partir de la cual se producen cambios profundos en el Derecho Internacional. De estos cambios, debe resaltarse la inclusión de los derechos del individuo en el ámbito internacional, a partir de la adopción de la Declaración Universal de los Derechos Humanos por parte de la Asamblea General de las Naciones Unidas, como respuesta a los horrores de la Segunda Guerra Mundial.

## El Desarrollo de las Tecnologías de la Información y la Comunicación en los Siglos XX y XXI y el Surgimiento de la "Personalidad Virtual"

Marcada por sus múltiples frentes, la Segunda Guerra Mundial finaliza en Europa con la muerte de Hitler y la posterior rendición Alemana el 7 de mayo de 1945 y en Asia el

9 de septiembre de 1945, con la rendición japonesa tras las explosiones nucleares de Hiroshima y Nagasaki.

En este contexto, la Segunda Guerra Mundial deja al mundo en una precaria posición al tiempo de su conclusión. El desarrollo de armamento nuclear, aunado con las tensiones existentes entre los países aliados (especialmente entre Estados Unidos y la Unión Soviética) al finalizar la Segunda Guerra, culmina con el inicio de un nuevo conflicto, esta vez de carácter ideológico, político, tecnológico y militar, conocido como "Guerra Fría".

A pesar de no llegar a constituirse como un conflicto bélico, la Guerra Fría marcó la segunda mitad del Siglo XX. Las tensiones políticas entre Estados Unidos y la Unión Soviética evolucionan hasta dividir el mundo en dos bloques de países contrapuestos, los cuales se enfrentaban por implementar sus respectivos modelos de gobierno en el ámbito global.

En el sentido ideológico, la Guerra Fría significó la contraposición de dos teorías fundamentales: la *capitalista*, sostenida por los Estados Unidos y los países miembros de la OTAN, y la *comunista*, aplicada por la Unión Soviética y los países aliados a ella. Tal dicotomía ideológica conllevó, tal como se mencionaba anteriormente, a la conformación de ejes que competían activamente entre sí por el control del planeta, lo cual tuvo consecuencias directas en la investigación y desarrollo de nuevas tecnologías, impulsadas por la siempre presente amenaza de una guerra nuclear.

Es el marco de la competencia entre ambas superpotencias, donde se hallan los inicios de la informática[13] moderna. Según Morales Viales y Ugarte Ibarra, *"Usualmente, el comienzo de la primera generación* (de ordenadores) *se sitúa en 1951, año de la fabricación del primer ordenador electrónico a escala industrial*" (Morales Viales & Ugarte Ibarra, 2012, pág. 10).

La producción de equipo computacional en grandes escalas se encontró originalmente dirigido hacia el desarrollo de tecnología bélica, lo cual se vio reafirmado cuando, en el año de 1957, la Unión Soviética lanzó y puso en órbita el primer satélite artificial (Sputnik). Tal hito significó el inicio de la "*carrera espacial*", verdadero ejemplo de la competencia entre las superpotencias aplicada hacia el control del espacio (percibido como una nueva frontera) y hacia la demostración de la superioridad ideológica de los respectivos bloques, manifestada en sus capacidades tecnológicas y de defensa.

Jorge Mújica, citado por Morales Viales y Ugarte Ibarra, recuerda que como respuesta a los logros obtenidos en materia aeroespacial por la Unión Soviética, el gobierno estadounidense dio inicio, en 1958, con su Agencia de Proyectos de Investigación Avanzada (ARPA por sus siglas en inglés) uno de sus proyectos; la llamada "ARPANET", *"un proyecto que desarrollaría la creación de una red de comunicación entre ordenadores. La particularidad de la iniciativa radicaba en la descentralización del sistema"* (Morales Viales & Ugarte Ibarra, 2012, pág. 11).

[13] Término que, en palabras de Riascos Gómez, fue acuñado por el francés Philippe Dreyfus y surge de la unión de "Información" y "automática". Según Davara y Arus es la "ciencia del tratamiento automatizado de la información" y que Riascos Gómez entiende como el "conjutno de reglas, principios y procedimientos teórico-técnicos que incardinados estudian las formas de recolección, selección, organización, tratamiento, almacenamiento y transferencia (por cesión o consulta) de los datos o informaciones de toda clase, tipo modalidad o fin, llevados a cabo por medios informáticos, electrónicos o telemáticos o por los que se llegaran a descubrir en el futuro" (Riascos Gómez, 1999).

Con el paso del tiempo, ARPANET se convirtió en el internet, una red global basada en *"la idea de que existirían múltiples redes independientes de diseño arbitrario, iniciando con la ARPANET como la red pionera"* (Leiner, y otros, 2009), lo cual se vio impulsado por los hitos que representaron la aparición del transistor en el año 1958; el desarrollo e implementación en masa de circuitos integrados a partir de 1964; el nacimiento del "miniordenador" y los lenguajes de alto nivel en 1965; y el desarrollo de los actuales sistemas computacionales en paralelo a partir de 1990 (Morales Viales & Ugarte Ibarra, 2012, pág. 13).

Esta evolución de la red, aunada con el abaratamiento y popularización de las tecnologías de la información y la comunicación, culminan con el surgimiento de la actual "*sociedad de la información*", en la cual las tecnologías que facilitan la *"creación, distribución y manipulación de la información juegan un papel esencial en las actividades sociales, culturales y económicas"* (Carrión, 2013). La sociedad de la información conduce al individuo a la utilización de las cada vez más ubicuas facilidades tecnológicas para la realización de una cantidad cada vez mayor de actividades diarias, para lo cual el individuo debe adoptar una "presencia virtual".

En este contexto surge en la actualidad el concepto de "*personalidad virtual*", el cual se constituye como la manifestación virtual de la personalidad individual; mediante ella el ser humano logra la extensión, tanto de su capacidad jurídica como de su dignidad individual al ámbito virtual, representado por las tecnologías de la información y la comunicación.

Así, el concepto de personalidad virtual representa *"el desdoblamiento del ser humano en su materialidad física y su desmaterialización virtual de información –principio de*

*ubicuidad–, donde esta personalidad virtual –conformada en forma absoluta de información*[14]*– se encuentra regulada por cada persona y será considerada como centro de atribución o imputación de efectos jurídicos"* (Chinchilla Sandí, 2005, pág. 5).

### *Derechos Humanos, Derechos Fundamentales y Derechos de la Personalidad*

A partir de la introducción histórica realizada, se ha podido analizar la manera en que, con el transcurso del tiempo, el ser humano ha sido dotado de valor y su personalidad ha sido reconocida como una prueba de su individualidad y, por consiguiente, como el origen de su dignidad.

Asimismo, se puede comprender ahora, de qué manera la personalidad humana se ha constituido para el individuo como *"su proyección en el ámbito jurídico, como una posibilidad abstracta para actuar como sujeto activo o pasivo en la infinita gama de acciones jurídicas" (Galindo Garfias, 1995, pág. 307)*, las cuales en la actualidad superan el plano terrenal y se elevan también a los nuevos mundos virtuales creados por la tecnología.

A pesar de lo anterior, sigue existiendo cierta confusión conceptual entre aquellos derechos que actualmente le son reconocidos al ser humano, especialmente en materia de los derechos subjetivos a los que hacen referencia los conceptos de "derechos humanos", "derechos fundamentales" y "derechos de la personalidad", los

[14] La cual se encuentra fragmentada en los diversos servicios que provee la sociedad de la información, tales como el email, las finanzas personales, las utilidades, el crédito, las redes sociales, los juegos en línea y los blogs, pese a lo cual puede ser "mapeada" dentro de diversas clasificaciones, tal como se estudiará en el siguiente capítulo. Un ejemplo gráfico de esta situación puede ser observado en el Anexo 3.

cuales han sido utilizados indistintamente por gran parte de la doctrina moderna, dado que estos tienden a solaparse *(Encabo Vera, 2012, pág. 20)*.

Es debido a tal confusión que se procederá a continuación, a la búsqueda de una delimitación entre unos y otros derechos, intentando aclarar sus elementos fundamentales, con miras a brindar al lector alguna claridad sobre el tema.

## Derechos Humanos

### *Definición*

Existen varias definiciones del concepto "derechos humanos", las cuales, como se verá ver más adelante, comparten ciertas características fundamentales. Zamora Hernández, en el capítulo titulado "Breve historia y teorías de los derechos humanos y los conflictos armados" de su tesis doctoral, presenta tres de ellas (Zamora Hernández, 2007), a saber:

*"El conjunto de prerrogativas inherentes a la naturaleza de la persona, cuya realización efectiva resulta indispensable para el desarrollo integral del individuo que vive en una sociedad jurídicamente organizada. Estos derechos, establecidos en la Constitución y en las leyes, deben ser reconocidos y garantizados por el Estado" – Comisión Nacional de Derechos Humanos, México.*

*"… los privilegios fundamentales que el hombre posee por el hecho de serlo, por su propia naturaleza y dignidad. Son derechos que le son inherentes y que, lejos de nacer de una*

*concesión de la sociedad política, han de ser consagrados y garantizados por ésta" –Antonio Trovel y Serra.*

*"… el conjunto de facultades, prerrogativas, libertades y pretensiones de carácter civil, político, económico, social y cultural, incluidos los recursos y mecanismos de garantía de todas ellas, que se reconocen al ser humano considerado individual y colectivamente" –Diccionario jurídico mexicano del IIJ de la UNAM.*

Por su parte, el Oxford Dictionary of Law los define como:

*"derechos y libertades de los cuales todo ser humano es titular. Protección contra afectaciones a estos derechos por un estado (incluyendo el estado del cual la víctima es nacional) puede en algunos casos ser obtenida en la ley internacional. Es algunas veces sugerido que los Derechos Humanos (o algunos de ellos) son tan fundamentales que forman parte de la ley natural, pero la mayoría de ellos son considerados como parte de la ley de los tratados"* [15] *(Martin, 2009).*

La Organización de las Naciones Unidas los define como:

"*Derechos inherentes a todos los seres humanos, sin distinción alguna de nacionalidad, lugar de residencia, sexo, origen nacional o étnico, color, religión, lengua, o cualquier otra condición" (Organización de las Naciones Unidas, 2012).*

Dicha definición encuentra su complemento en la definición dada por la Unión Inter-Parlamentaria, la cual, en su "Human Rights Handbook for Parlamentarians", establece que:

[15] Human rights: Rights and freedom to which every human being is entitled. Protection against breaches of these rights by a state (including the state of which the victim is a national) may in some cases be enforced in international law. It is sometimes suggested that human rights (or some of them) are so fundamental that they form part of natural law, but most of them are best regarded as forming part of treaty law.

"los Derechos Humanos son la suma de los derechos individuales y colectivos establecidos en las constituciones estatales y la ley internacional (…) son derechos que todo ser humano tiene por virtud de su dignidad humana" (Inter-Parliamentary Union, 2005).

A partir de todas las definiciones citadas, es posible comprender entonces a los Derechos Humanos como *el conjunto de derechos inherentes a la persona humana por el mero hecho de serlo, por lo que no dependen de su reconocimiento por los Estados para ser atribuibles a todo ser humano*[16].

### *Fundamentos*

Los derechos humanos, representan según Nikken una *"ideología universal nacida para encarar la opresión"*, la cual se fundamenta en la concepción de estos derechos como un concepto dinámico. Este concepto no nace a partir de las leyes, designios o concesiones estatales, sino que surge a partir de atributos humanos que preceden cualquier garantía estatal y, a partir de la afirmación de la dignidad de la persona

[16] Esta definición se encuentra dirigida a enfocar los derechos humanos como el grado más amplio de la escala formada por los derechos analizados durante la presente investigación; entra en esta categoría una serie de postulados generalísimos similares a los derechos iusnaturales en tanto podrán ser revelados por la razón humana.
En este punto deben realizarse dos aclaraciones:

1) En tanto la definición provista es evidentemente abierta, propongo el consenso por la mayor parte de los países del orbe como parámetro para su reconocimiento mundial (para lo cual necesariamente debemos hacer referencia a la Organización de las Naciones Unidas como único ente capaz de determinar tal consenso).
2) Esta definición deja de lado por supuesto el tema de la efectividad de los derechos humanos, los cuales dependen efectivamente de su reconocimiento por parte de los estados para ser exigibles por los habitantes de dicho estado. Este es un elemento externo a la definición de los Derechos Humanos y, tal como establece Trovel y Serra y la Comisión de Derechos Humanos de México, será deber de los Estados reconocer y garantizar dichos derechos.

frente al Estado, se constituyen como causa de reforma "contra leyes opresivas que los desconocían o menoscababan" (Nikken, 2010, pág. 55).

Tales atributos conforman la dignidad humana, por lo cual los derechos humanos no pueden ser condicionados por elementos externos al individuo. Al respecto, Lozano afirma que, *"si toda persona es portadora de una dignidad, de esa dignidad derivan necesariamente unos bienes jurídicos que se le atribuyen como algo propio de la persona, el título que convierte a esta en titular de derecho, en portadora de derechos dada su condición humana" (Lozano, 2009, pág. 47).*

En tanto encuentran sus bases en la dignidad humana, y dado que debe considerarse necesariamente a *"toda persona como ser humano y a todo ser humano como persona" (Nikken, 2010)*, los derechos humanos se constituyen en verdaderos *"bienes jurídicos subjetivos independientemente de que se encuentren reconocidos en el ordenamiento jurídico"* (Lozano, 2009, pág. 41) cuyo valor será, por tanto, supralegal.

### *Principios*

La doctrina señala que los derechos humanos comparten, dentro de su definición misma, algunos principios que se constituyen como sus elementos básicos alrededor del eje central que constituye la persona humana. Algunos de estos principios son:

a) Principio de Universalidad o Generalidad: Al encontrarse basados en la dignidad humana, y al ser aceptados por la gran mayoría de los Estados y culturas, los derechos humanos se constituyen como universales. *(Inter-*

*Parliamentary Union, 2005, pág. 4).* Debiendo ser aplicados en igualdad de condiciones y sin discriminación alguna a todos los seres humanos, se constituyen como derechos "*erga omnes" (Nino, 2009, pág. 20).*

b) Principio de Historicidad: Comprende el origen múltiple del concepto de derechos humanos y relaciona la manifestación y protección de tales derechos a *"situaciones históricas y necesidades humanas concretas" (Lozano, 2009, pág. 38).*

c) Principio de Inalienabilidad: El cual establece que ningún ser humano puede ser despojado de sus derechos humanos, salvo en aquellas situaciones claramente establecidas por la ley *(Inter-Parliamentary Union, 2005, pág. 4).*

d) Principio de Positividad: Comprende la necesidad de realizar una positivización de los derechos humanos con miras a asegurar su protección, pero da a tal positivización, carácter declarativo, no constitutivo *(Lozano, 2009, pág. 40).*

*e)* Principio de Dignidad de la Persona: Este principio *"prescribe tratar a los hombres de acuerdo con sus voliciones y no en relación con otras propiedades sobre las cuales no tienen control" (Nino, 2009, pág. 20).*

f) Principio de Permanencia: Establece que todo ser humano debe gozar de la protección brindada por los derechos humanos desde el momento de su concepción hasta el de su muerte (Zamora Hernández, 2007, pág. 24).

g) Principio de Facultatividad: Considera a los derechos humanos como *"prerrogativas pertenecientes a la persona y que permiten exigir del Estado o de otras personas, abstenciones o prestaciones"* (Lozano, 2009, pág. 37).

*h)* Principio de autonomía de la persona: Da valor a la *"persecución de planes de vida e ideales de excelencia (y, en virtud de un principio complementario, al placer y a la ausencia de dolor)" (Nino, 2009, pág. 20).*

i) Principio de Imprescriptibilidad: Comprende que los derechos humanos no se ven afectados por el paso del tiempo o circunstancia alguna que normalmente afecte a otros derechos *(Zamora Hernández, 2007, pág. 23).*

j) Principio de Incondicionalidad: La titularidad de los derechos humanos no se encuentra condicionada a la posesión de característica alguna, comprendiéndose que únicamente se encuentran supeditados a *"los límites de los propios derechos, es decir, hasta donde comienzan los derechos de los demás o los justos intereses de la comunidad" (Zamora Hernández, 2007, pág. 26).*

*k)* Principio de inviolabilidad de la persona: El cual *"prohíbe imponer sacrificios a un individuo sólo en razón de que ello beneficia a otros individuos" (Nino, 2009, pág. 20).*

### *Clasificaciones*

Dado el tratamiento tradicionalmente multidisciplinario que ha tenido el tema de los derechos humanos, actualmente resulta imposible afirmar la existencia de una única forma de clasificación.

Al respecto, Aguilar Cuevas señala la existencia de por lo menos tres maneras en que tal clasificación ha sido realizada, a saber: mediante un enfoque historicista (que busca demostrar la existencia de una protección que aumentó progresivamente a lo largo de

la historia); mediante un enfoque de jerarquía (que busca clasificar los derechos humanos diferenciando entre derechos llamados "esenciales" y derechos "complementarios"); y mediante un enfoque periódico (caracterizado por el uso de las famosas tres generaciones de cobertura progresiva) *(Aguilar Cuevas, 1998, pág. 93)*, al cual se dará especial atención, dado que es el más conocido en nuestro medio.

El enfoque periódico se caracteriza por diferenciar el desarrollo de los derechos humanos en tres generaciones, las cuales responden a diversos contextos históricos y protegen intereses progresivamente más amplios.

- Primera Generación

La primera y más antigua de las generaciones de este enfoque periódico surge a partir de la Revolución francesa como respuesta al absolutismo que exige el establecimiento y respeto por parte del Estado, de derechos fundamentales inherentes al individuo, los cuales poseen una naturaleza fundamentalmente civil y política.

Aguilar Cuevas indica que los derechos de esta primera generación se caracterizan por imponer "*al Estado el deber de respetarlos siempre*" *(Aguilar Cuevas, 1998, pág. 94)*; su naturaleza los dirige a proteger de los excesos estatales al individuo, el cual se constituye en titular de tales derechos, por lo cual le asiste la facultad de reclamarlos.

Dentro de esta generación tradicionalmente han sido enmarcados, entre otros, los derechos a continuación detallados:

- Derecho a tener derechos y libertades fundamentales
- Derecho a la vida, libertad y seguridad jurídica

- Derecho a la Igualdad
- Derecho a la privacidad e intimidad
- Derecho a no ser molestado arbitrariamente en su vida privada, su familia, su domicilio o correspondencia, ni con ataques a su honra o reputación
- Derecho a la libre circulación por territorio nacional
- Derecho a la nacionalidad
- Derecho a solicitar asilo
- Derecho a contraer matrimonio y derecho a procrear
- Libertad de pensamiento y religión
- Libertad de opinión y expresión
- Libertad de reunión y asociación pacífica
- Derecho al reconocimiento de personalidad jurídica
- Derecho a exigir igualdad ante la ley
- Derecho de amparo
- Derecho a ser juzgado por un tribunal imparcial
- Derecho a participar en el gobierno y derecho a ocupar un cargo público
- Derecho al voto
- Derecho a no ser detenido de manera arbitraria
- Derecho a gozar de la presunción de inocencia

- Segunda Generación

Constituida por derechos sociales, económicos y culturales, surgen como respuesta a la Revolución Industrial, *"por medio de los cuales el estado de Derecho pasa a una etapa*

*superior, o sea a un Estado Social de Derecho, donde se demanda un Estado de Bienestar que imponga programas, acciones y estrategias para lograr un goce total de las personas" (Zamora Hernández, 2007, pág. 28).*

Según indica Aguilar Cuevas, debido a su carácter colectivo, los derechos que se incluyen dentro de esta segunda generación buscan ampliar *"la esfera de responsabilidad del Estado"*, para lo cual se establece un deber hacer positivo por parte del Estado hacia el titular, cual es el individuo en comunidad, quien se asocia para su defensa y para la defensa de las *"legítimas aspiraciones de la sociedad"* (Aguilar Cuevas, 1998, pág. 96).

Normalmente se considera que, si bien todo Estado debe satisfacer las obligaciones que le impone esta segunda generación de derechos, tal obligación se encuentra condicionada a las posibilidades económicas de cada país.

Dentro de esta segunda generación normalmente se encuentran plasmados derechos como:

- Derecho a la seguridad social y satisfacción de derechos de segunda generación
- Derecho al trabajo
- Derecho a formar sindicatos
- Derecho a un nivel de vida adecuado
- Derecho a la salud física y mental
- Derecho a cuidados y asistencia durante maternidad e infancia
- Derecho a la educación
- Derecho a la seguridad pública

- Tercera Generación

La tercera generación de derechos humanos hace referencia a los llamados "derechos de los pueblos" o "derechos de solidaridad", los cuales son creados *"para aumentar y promover el progreso social y elevar el nivel de vida de todos los pueblos, en un contexto de respeto y colaboración mutua entre las distintas naciones de la comunidad internacional"* (Zamora Hernández, 2007, pág. 28).

Según Aguilar Cuevas, estos derechos responden "a la necesidad de cooperación entre las naciones o grupos", por lo que puede asegurarse que pertenecen *"a grupos imprecisos de personas con un interés colectivo común"*, que requiere de prestaciones positivas o negativas por parte de un Estado o de toda la Comunidad Internacional (Aguilar Cuevas, 1998, pág. 98). Los derechos comprendidos por esta tercera generación son, entre otros:

- Derecho a la autodeterminación de los pueblos
- Derecho a la independencia económica y política
- Derecho a la identidad nacional y cultural
- Derecho a la paz
- Derecho a la coexistencia pacífica
- Derecho a la cooperación internacional y regional
- Derecho al desarrollo
- Derecho a la justicia social internacional
- Derecho al uso de avances de ciencias y tecnología
- Derecho al medio ambiente

- Derecho al patrimonio común de la humanidad
- Derecho al desarrollo

## Derechos Fundamentales o Garantías Individuales

### *Definición*

El concepto de derechos fundamentales a menudo es confundido con el concepto de derechos humanos. La razón de ello puede encontrarse en que, tal como se estudió anteriormente, los derechos humanos de primera generación son por lo general comprendidos como garantías fundamentales inherentes al individuo.

A pesar de lo anterior, la existencia de diferencias entre uno y otro concepto es generalmente aceptada por la doctrina, lo cual se denota en las diversas definiciones que sobre derechos fundamentales se han encontrado, en las cuales se enfatizan diferencias en aspectos como la fundamentación y requisitos que se establecen para ser titular de derechos fundamentales.

Burgoa Orihuela, citado por De la Parra Trujillo, señala que:

*"las garantías individuales son las relaciones jurídicas de supra a subordinación que se establecen entre el gobernado, por un lado, y cualquier autoridad y el Estado, por el otro; relación de la que surge un derecho subjetivo a favor del gobernado y un deber para el Estado y sus Autoridades consistente en respetar ese derecho del gobernado; teniendo como fuente la Constitución Política"* (De la Parra Trujillo, 2001, pág. 153).

Nogueira Alcalá, citado por Arias Cordero y Chaves Rodríguez los entienden como aquellos:

*"derechos, libertades, igualdades o inviolabilidades que, desde la concepción, fluyen de la dignidad humana y que son intrínsecos de la naturaleza singularísima del titular de esa dignidad. Tales atributos, facultades o derechos públicos subjetivos son, y deben ser siempre, reconocidos y protegidos por el ordenamiento jurídico, permitiendo al titular exigir su cumplimiento con los deberes correlativos"* (Arias Cordero & Chaves Rodríguez, 2010).

Por su parte, Arias Cordero y Chaves Rodríguez definen los derechos fundamentales como:

*"El conjunto de derechos y libertades jurídicas reconocidos y garantizados por el Derecho positivo y que sirven de base para la totalidad del sistema estatal*. (…) *son derechos que el poder estatal reconoce y protege aunque se ejercen en el ámbito de las Relaciones privadas (en su origen) transformándose en públicas desde el momento en que forman parte del derecho positivo"* (Arias Cordero & Chaves Rodríguez, 2010).

Por otro lado, Luigi Ferrajoli, brinda la definición que a juicio del suscrito autor de esta investigación, es la más acertada del término, en la cual establece que:

"(…) son "derechos fundamentales" todos aquellos derechos subjetivos que corresponden universalmente a "todos" los seres humanos en cuanto dotados del status de personas, de ciudadanos o personas con capacidad de obrar; entendiendo por "derecho subjetivo" cualquier expectativa positiva (de prestaciones) o negativa (de no sufrir lesiones) adscrita a un sujeto por una norma jurídica; y por "status" la condición de un sujeto, prevista asimismo por una norma jurídica positiva, como presupuesto de su idoneidad para ser titular de situaciones jurídicas y/o autor de los actos que son ejercicio de éstas" (Ferrajoli, 2004, pág. 37).

A partir del estudio de la totalidad de las definiciones anteriormente presentadas, es posible comprender entonces que el concepto de derechos fundamentales hace referencia a aquel conjunto de derechos subjetivos y libertades reconocidos a toda persona por las normas jurídicas imperantes en cada Estado.

De esta manera, el concepto de derechos humanos acompasa un conjunto de derechos inherentes a toda persona con independencia del reconocimiento que de estos realizara un Estado determinado; mientras que el concepto de derechos fundamentales limita este conjunto de derechos subjetivos a aquellos reconocidos oficialmente por el Estado en que se encuentre el individuo, pudiendo estos corresponder o no con respecto al conjunto de derechos humanos vigentes en el ámbito internacional en cada momento histórico[17].

### *Fundamentos*

En su texto, *"Sobre los Derechos Fundamentales",* el profesor Ferrajoli, continúa explorando la definición anteriormente expuesta y expone los aspectos que considera como base de su concepción de derechos fundamentales; a saber, "*la indisponibilidad o inalienabilidad*" (Ferrajoli, Sobre los Derechos Fundamentales, 2006, pág. 117) de los

[17] Pueden encontrarse diversos ejemplos de esta situación en el ámbito internacional, resultando fundamentalmente evidente la disparidad entre los derechos humanos y los derechos fundamentales reconocidos en cada Estado con tan solo examinar la manera en que son tratados algunos temas polémicos por los marcos normativos de los diferentes Estados.
Así, en la actualidad pueden ser encontrados múltiples ejemplos de Estados que no reconocen dentro del conjunto de derechos fundamentales de sus habitantes derechos Humanos como los derechos a la libertad, a no vivir bajo la tortura, o a no ser víctima de la discriminación.

derechos, una vez que han sido brindados a un individuo por la Constitución Política de su país, la cual se constituye en fuente de tales derechos.

A pesar de sostener tal *"indisponibilidad e inalienabilidad"* como parte teórica del concepto de derechos fundamentales, el profesor Ferrajoli expresa también que:

"*son "fundamentales" los derechos adscritos por un ordenamiento jurídico a todas las personas físicas en cuanto tales, en cuanto ciudadanos o en cuanto capaces de obrar. Pero diremos también, sin que nuestra definición resulte desnaturalizada, que un determinado ordenamiento jurídico, por ejemplo totalitario, carece de derechos fundamentales. La previsión de tales derechos por parte del derecho positivo de un determinado ordenamiento es, en suma, condición de su existencia o vigencia en aquel ordenamiento, pero no incide en el significado del concepto de derechos fundamentales"* (Ferrajoli, Derechos y garantas, la ley del más débil, 2004, pág. 37).

Así, Ferrajoli reconoce también la dependencia de titularidad del individuo sobre derechos fundamentales, al reconocimiento que de estos derechos realice el Estado, lo cual implica además que estos derechos se manifestarán en el ser humano solamente en tanto se le reconozca como "ciudadano", "persona" o "persona con capacidad de obrar".

### *Características*

Con respecto a las características de los derechos fundamentales, resulta conveniente hacer referencia al trabajo de De la Parra Trujillo, quien señala tres características de

las garantías individuales, las cuales vale la pena resaltar. Tales características se encuentran fundamentalmente relacionadas con los sujetos involucrados y su finalidad (De la Parra Trujillo, 2001).

Como primera característica, De la Parra Trujillo apunta al hecho de que en estos derechos el sujeto activo es *"el gobernado"*, mientras que los derechos humanos tienen como sujeto activo a todo ser humano.

Una segunda característica señalada por el autor puede encontrarse en el sujeto pasivo de estos derechos, el cual no es otro que el *"Estado y sus autoridades"*, lo cual incluye a los organismos paraestatales que se encuentren en *"relación de supra a subordinación".*

La tercera característica se encuentra relacionada profundamente con las dos anteriores, en tanto el autor reafirma la posición doctrinaria que sostiene a la Constitución Política de cada país como fuente de los derechos fundamentales y señala como finalidad de estos la *"protección de la dignidad humana para el pleno desarrollo de la personalidad de las personas físicas, ya sea directamente o indirectamente a través de las personas morales"* (De la Parra Trujillo, 2001, pág. 154).

## Derechos de la Personalidad

Tratados fundamentalmente por el Derecho Civil, los derechos de la personalidad han sido caracterizados tradicionalmente dentro del Derecho Privado como la manifestación positiva de aquellos derechos humanos de primera generación que se

dirigen hacia la defensa del derecho humano del pleno desarrollo de la personalidad y de aquellos rasgos de la personalidad que constituyen la dignidad individual.

Si bien presentan algunas similitudes con los derechos humanos, el tratamiento dado por la doctrina a los derechos de la personalidad por lo general ha sostenido que tal equiparación no resulta conveniente. Desde el punto de vista tradicional, los derechos humanos han sido contrapuestos con los derechos de la personalidad, en tanto que, mientras los primeros buscan regular el desarrollo de la personalidad individual en el Derecho Público, los segundos han sido dirigidos hacia la defensa de la personalidad y la individualización del sujeto en el marco del Derecho Privado.

### *Definición*

Existen diversas definiciones aplicables a los derechos de la personalidad, las cuales presentan variaciones significativas en su especificidad y en la perspectiva que sobre el concepto presentan al lector.

Algunas de ellas, tales como las realizadas por Ferrara, citado por Galindo Garfias, y por Domínguez Guillén, presentan el concepto de manera amplia:

*"los Derechos de la Personalidad son aquellos que "Garantizan el goce de nosotros mismos, aseguran al individuo el señorío de su persona, la actuación de sus propias fuerzas físicas y espirituales"* (Galindo Garfias, 1995).

*"Los derechos de la personalidad son aquellos que protegen civilmente la esencia física y moral de la persona. Estos permiten que el sujeto de derecho despliegue la plenitud de valores que*

*reclama su status y por si mismos conforman la máxima garantía que supone la condición plena de ser persona"(Domínguez Guillén, 2003, pág. 4).*

Por otra parte, Encabo Vera presenta al lector con una definición más centrada, la cual establece que estos derechos:

"(…) constituyen, en definitiva, manifestaciones, tanto exteriores como interiores, diversas de la cada persona singular, su dignidad y su propio ámbito individual. También podemos decir que los derechos de la personalidad son aquellos que el ordenamiento jurídico concede para la protección de los intereses más personales de un individuo, de ahí la justificación de tal denominación" (Encabo Vera, 2012, pág. 15).

De la misma manera, Enrique Gutiérrez y González, citado por De la Parra Trujillo, los define como:

*"(…) los bienes constituidos por determinadas proyecciones, físicas y psíquicas del ser humano, relativas a su integridad física y mental, que las atribuye para sí o para algunos sujetos de derecho, y que son individualizadas por el ordenamiento jurídico"(De la Parra Trujillo, 2001, pág. 141).*

Esta última definición es retomada por, Ernesto Romero González, quien establece en su trabajo "*Los derechos de la Personalidad"*, que serán comprendidos como derechos de la personalidad *"los derechos subjetivos previstos por el ordenamiento jurídico positivo, que tutelan la dignidad de la persona, a través de la protección de ciertos bienes constituidos por proyecciones físicas o psíquicas del ser humano, atribuidas para sí u otros sujetos de derecho" (De la Parra Trujillo, 2001, pág. 41).*

Consideramos, junto con De la Parra Trujillo, que esta última definición resulta superior a las anteriores, esto debido a que, si bien todas las definiciones expuestas

comunican en mayor o menor medida el valor que protegen estos derechos, la definición de Romero González *"hace referencia a la naturaleza jurídica de los derechos de la personalidad, los emancipa de la Doctrina del Derecho Natural, determina su finalidad y los objetos que protegen, así como su sujeto activo"* (De la Parra Trujillo, 2001, pág. 41).

### *Fundamentos*

En tanto los derechos de la personalidad han sido tratados tradicionalmente desde el punto de vista del Derecho Civil, resulta posible establecer que se encuentran fundamentados principalmente en la legislación interna de cada país y surgen a partir de los principios establecidos por su respectiva Constitución Política.

Tal como se estudiara con anterioridad, los derechos de la personalidad han tenido mayor o menor importancia a lo largo del tiempo, a pesar de lo cual su protección por parte del Derecho es relativamente reciente (Encabo Vera, 2012, pág. 18), y aún en su corta vida, la teoría detrás de tal protección se ha caracterizado por contar con posiciones encontradas en la doctrina.

A pesar de lo anterior, un estudio de la evolución presentada por los derechos de la personalidad en los diversos sistemas jurídicos puede detectar caracteres análogos. En este sentido, Morales Godo manifiesta que, si bien en algunos casos el desarrollo de estos derechos se encontró fundamento en el Derecho Privado y en otros en el Derecho Constitucional, su relación con la dignidad humana permite afirmar que *"En términos genéricos, todas las garantías constitucionales pueden ser entendidas como derechos*

*de la personalidad y dan lugar a protección civil" (Morales Godo, Instituciones del Derecho Civil, 2009, pág. 536).*

De Lama Aymá, en su tesis doctoral titulada *"La protección de los derechos de la personalidad del menor de edad" (De Lama Aymá, 2004)* realiza una breve caracterización de las teorías que fundamentan los actuales derechos de la personalidad, en la cual recuerda al lector la existencia de tres posiciones doctrinales que en sus discusiones sobre el tema sostenían tesis diferentes.

La primera de estas tesis, conocida como *tesis monista*, sostenía la necesidad de que el Derecho positivo protegiera un único Derecho general a la personalidad dado que consideraba que *"éste es un valor unitario de imposible fraccionamiento en múltiples situaciones jurídicas*" *(De Lama Aymá, 2004)*. El principal fundamento de esta tesis se encontraba en considerar que resultaría imposible para el Derecho velar por las distintas manifestaciones de la personalidad en caso de que estas fueran establecidas individualmente por la ley (puesto que sería imposible que la ley incluyera la totalidad de aspectos relevantes a la personalidad).

La segunda teoría, la *tesis pluralista*, consideraba como mejor respuesta a la necesidad de proteger la personalidad, el establecimiento positivo de cada una aquellas manifestaciones de la personalidad que el Derecho consideraba dignas de protección. El fundamento de esta teoría se encontraba en la seguridad jurídica que brindaba al individuo el poseer derechos reconocidos de forma expresa, lo cual sería difícilmente lograble si se contara con un solo derecho genérico a la protección de la personalidad que debiera ser interpretado por un juez.

Es con las llamadas *tesis mixtas* que el problema encuentra finalmente una solución al proponer estas la inclusión en el ordenamiento jurídico de un derecho general a la personalidad y de una pluralidad de derechos que velaran por manifestaciones específicas de la personalidad.

Estas tesis mixtas encuentran sus primeras manifestaciones en los códigos civiles de Alemania y de Portugal, a inicios del Siglo XX y alcanzan gran popularidad dado que presentan un nivel adecuado de protección aunado con suficiente flexibilidad como para adaptarse a los diversos casos. A pesar de esto, ya desde sus inicios, encuentran un obstáculo en su dependencia en el sujeto para su protección, al considerar la protección de la personalidad como un derecho subjetivo solamente defendible en el ámbito privado, por medio del derecho de daños (Encabo Vera, 2012, pág. 19).

Tal como lo establece la definición de Romero González, los derechos de la personalidad poseen aún hoy un carácter fundamentalmente *subjetivo* (dado que corresponde al individuo velar y exigir al Estado su defensa y tutela); el cual busca tutelar la dignidad del individuo manifestada en su *personalidad* (comprendida en este caso como el conjunto de "rasgos biológicos, sociológicos y psicológicos que son consustanciales a cada persona en su devenir desde su nacimiento") (Encabo Vera, 2012, pág. 16).

A pesar de lo anterior, a partir de la Segunda Guerra Mundial es lograda una unificación en la protección brindada por los derechos de la personalidad y los derechos fundamentales a partir de la percepción de que "*no es aceptable que en un Estado de Derecho la enumeración de derechos fundamentales no recoja todos los derechos de la personalidad porque no es pensable que los derechos más inherentes a la persona, los de la*

*personalidad, no tengan reconocida la protección máxima del ordenamiento jurídico mediante su elevación a rango fundamental"* (De Lama Aymá, 2004, pág. 26).

De esta manera, actualmente es posible afirmar que la defensa de los derechos subjetivos comprendidos por los derechos de la personalidad puede ser extendida al ámbito público e incluso penal (Encabo Vera, 2012, pág. 19). Así, el Estado mismo ha visto cambiar su rol en la defensa de los derechos de la personalidad, abandonando su papel de mero agresor de los derechos individuales, para constituirse hoy también en defensor del individuo ante agresiones provenientes de entes públicos y privados por igual.

Ante la actual coexistencia de Derecho Público y Derecho Privado, los derechos de la personalidad adquieren nuevas dimensiones, por lo que hoy son observados como sujetos a una naturaleza dual de derechos subjetivos (siempre a disposición del individuo) y, a la vez, de bienes o valores superiores, tutelados por el ordenamiento en general y considerada su protección parte fundamental del interés público[18].

### *Características*

[18]*En palabras de De Lama Aymá,* "Entender la personalidad como un valor superior del ordenamiento del cual emanan todos los derechos de la personalidad nos permite superar la dificultad que entraña partir únicamente de una pluralidad de derechos reconocidos por el ordenamiento jurídico, a saber, que ante una regulación o reconocimiento escaso e incompleto de los mismos, la personalidad queda desprotegida. Y al mismo, tiempo nos permite escapar de la figura del derecho subjetivo cuando ésta no nos proporciona la protección de la personalidad que exige un Estado de Derecho" (De Lama Aymá, 2004, pág. 33).

Usualmente los derechos de la personalidad son identificados con ciertas características generales, las cuales han sido compiladas y tratadas tanto por Domínguez Guillén como por De la Parra Trujillo, por lo que seguidamente procederá su enunciación:

- Son derechos subjetivos (por lo que parten de un permiso brindado por el Estado a su titular; imponen un deber a los demás de no interferir; derivan de una norma jurídica que los establece y brindan al titular la capacidad de exigir el cese de toda afectación o interferencia en su disfrute por terceros)
- Su titular generalmente es una persona física, pero hay algunos de ellos que pueden pertenecer a personas morales.
- Son patrimoniales pero no pecuniarios (forman parte del patrimonio moral de todo individuo).
- Son personalísimos, pues por lo general nacen y se extinguen con la persona y solo pueden ser ejercitados por su titular.
- Varían de época en época y de sociedad en sociedad.
- Son absolutos, oponibles erga omnes.
- Son intransmisibles.
- Son irrenunciables.
- Son inembargables.
- Son imprescriptibles.

### *Clasificaciones*

De conformidad con lo anteriormente mencionado, la existencia de un derecho general a la protección de la personalidad es comúnmente aceptada en la actualidad. Tal concepto general se encuentra directamente ligado con los conceptos de dignidad humana que fundamentan tanto los derechos fundamentales como los derechos humanos.

A pesar de lo anterior, la existencia de derechos específicos de la personalidad que se encuentran dirigidos a la protección de ciertas manifestaciones de esta, es también aceptada tanto por la doctrina como por la jurisprudencia de gran cantidad de países.

Estos derechos específicos pueden ser clasificados de diversas maneras según el contexto legal de cada país; sin embargo, en términos generales, puede establecerse que los derechos comprendidos dentro de los derechos de la personalidad son los siguientes (Domínguez Guillén, 2003):

- Derecho a la identidad: No solamente establece el derecho a tener un nombre sino que se extiende al derecho a ser "único e irrepetible". Este derecho se encuentra conformado por un elemento físico (identidad estática) y un elemento dinámico (identidad y patrimonio cultural del sujeto), los cuales, según Domínguez Guillén, pueden ser vulnerados *"cuando se afecta la verdad biográfica de una persona, alteración u omisión de hechos o circunstancias fundamentales que conforman el perfil social del sujeto y que éste tiene interés en preservar, porque, en su conjunto, eso es lo que lo hace un ser único"* (Domínguez Guillén, 2003, pág. 8).

- Derechos relativos al cuerpo: Clasificación que según Domínguez Guillén puede caracterizarse por su relación con la integridad física o corporal del individuo; dentro de los cuales se encuentran los siguientes:
  - *Derecho a la Vida* (o derecho a seguir viviendo): Dentro del cual se estudian algunos derechos aun controversiales, tales como el suicidio, la eutanasia (o derecho a morir sin dolor), la ortotanasia (o derecho a morir con dignidad), el derecho a la integridad física, entre otros.
  - *Derecho a la Integridad Física*: Dentro del cual la autora señala los derechos a negarse a un examen corporal y a no ser sometido a experimentos sin la voluntad del interesado.
  - *Derecho a la Libre Disposición del Cuerpo:* Complementa la integridad corporal y permite al individuo disponer (dentro de los límites legales establecidos en su país) de su cuerpo; se incluyen dentro de este derecho temas como la negativa a practicarse operaciones quirúrgicas, el trasplante de órganos, e inclusos derechos de mayor actualidad que aún son discutidos, tales como la modificación genética del individuo.
- *Derechos relativos a la integridad moral:* Clasificación que en criterio de Domínguez Guillén incluye aquellos derechos relacionados con los aspectos morales del individuo, dentro de los cuales se encuentran los siguientes:
  - *Derecho a la Libertad*: Constituido por la posibilidad de escoger o seleccionar; tradicionalmente relacionado con el "libre albedrío" que debe caracterizar al ser humano, permite al sujeto *"desplegar la plenitud de su autodeterminación"* (Domínguez Guillén, 2003, pág. 11) e incluye multiplicidad de libertades.

- *Derecho al Honor*: Posee un doble ámbito, subjetivo (sentimiento de apreciación de nuestra dignidad) y objetivo (forma en que los terceros captan esta).
- *Derecho a la Intimidad:* Entendido usualmente como aquel que permite al ser humano poseer un ámbito de su persona que puede reservar u ocultar de los demás
- *Derecho a la Privacidad:* Identificado por el derecho anglosajón como el "Derecho a no ser molestado".
- *Derecho a la Autodeterminación Informativa:* Contrapuesto tradicionalmente al derecho a la información en tanto este procura brindar al individuo control sobre su información.
- *Derecho a la Imagen:* Identificado con los "*Personality Rights"* del derecho anglosajón, procura brindar control al individuo sobre la representación gráfica de su figura y el uso comercial de esta.
- Derecho de *Voz:* Similar en su protección al derecho a la imagen, protege la representación sonora del individuo ante usos comerciales no autorizados.

## *Síntesis de la Primera Sección*

Breve Introducción Histórica

*A lo largo de la cual se detalla el proceso histórico que ha dado lugar al reconocimiento de los derechos humanos, fundamentales y de la personalidad.*

- El concepto de derechos del hombre como conjunto de prerrogativas del gobernado de observancia jurídica obligatoria e imperativa, para los gobernantes resulta ajeno a la mayor parte de las sociedades antiguas. Igual situación existe con respecto a la protección de la intimidad, dada la extrema sumisión del individuo a los usos y costumbres de su pueblo, las cuales se extendían incluso a los ámbitos más privados de su vida.
- En la sociedad de la Grecia Clásica son logrados marcados avances hacia la participación ciudadana en el gobierno de la ciudad, con la implementación de la democracia como sistema político.

  Esta innovación, aunada con la gran labor filosófica de los pensadores de la época, constituye uno de los primeros ejemplos de esfuerzos tendientes hacia la dignificación de la persona humana por parte de una sociedad. A pesar de ello esta sociedad no logra mayores avances en cuanto a la protección de la intimidad individual, dada la intrínseca relación del individuo con su comunidad.
- La sociedad romana fue caracterizada en sus etapas tempranas por reconocer derechos y ciudadanía únicamente al *pater familias*, quien se constituía como amo y señor sobre los integrantes de su familia. Esta situación cambia a lo largo de la historia romana hasta que finalmente es otorgada la ciudadanía a todos los individuos libres.

  Igual evolución se da en el pensamiento romano, en el cual individuos como Cicerón y Gayo postulan las primeras ideas iusnaturalistas; se reconoce durante esta época la existencia de dos derechos: el tradicional *Ius Civile* y un nuevo derecho: el *Ius Gentium*, revelado por la razón y común a todos los pueblos.
- La Edad Media se encuentra marcada por la ruptura del tradicional absolutismo del Estado, a favor de una sociedad basada en una relación de semidependencia entre el un individuo semilibre y su señor feudal. Esta ruptura del absolutismo puede

verse representada, entre otros eventos, por la firma de la *Carta Magna de las Libertades* en la cual el monarca acepta limitar sus poderes frente a sus súbditos.

En el plano ideológico esta etapa se caracteriza por la evolución del iusnaturalismo, surgiendo así la concepción eclesiástica del Derecho natural, representada por la Patrística y la Escolástica, basadas en la noción de dignidad humana universal, con fundamento en la voluntad divina.

- El Renacimiento conlleva un retorno a las ideas clásicas como las de estado-ciudad (con autores como Maquiavelo) y a los modelos de gobierno absolutistas, lo cual es seguido por una lenta pero constante evolución del pensamiento a favor de la dignidad y las libertades humanas.

  Esta evolución culmina en el siglo SVII con el asentamiento de las bases para la doctrina de los derechos del hombre y del ciudadano, por los integrantes de la *Escuela del Derecho Natural.* Por otro lado, se encuentran también en este siglo los fundamentos para la actual teoría de los derechos de la personalidad, en las obras de autores como Gómez de Amescúa y Strick.
- El siglo XVIII reviste una gran importancia histórica. Su principal movimiento (la Ilustración) se caracteriza por dar énfasis a la información y a la libertad de prensa como respuesta contra la ignorancia, la superstición y la tiranía. La Ilustración culmina en 1789 con la Revolución francesa y la posterior Declaración de los Derechos del Hombre y el Ciudadano, fundamento de las revoluciones de los siglos posteriores y de nuestro actual concepto de derechos humanos.
- A pesar del ímpetu causado por la Ilustración y la Revolución francesa, el siglo XIX se encuentra marcado por el pensamiento individualista y liberal y el declive del iusnaturalismo. A pesar de encontrar en este siglo algunos ejemplos de declaraciones que ya contemplan los derechos inherentes a las personas, dados los efectos de la Revolución Industrial el siglo XIX puede ser caracterizado por la inequidad social.

  Esta situación tiene como consecuencia el desarrollo del concepto de dignidad humana y teorías paralelas que afirmaban la posesión por el individuo de un derecho a su propia personalidad.

- El siglo XX se ve marcado, desde sus inicios, por las dos guerras mundiales y es debido a los profundos efectos de ambas guerras que da inicio un movimiento mundial dirigido al establecimiento de mecanismos internacionales capaces de evitar la repetición de tales hechos. Este movimiento culmina en 1945 con la fundación de la Organización de las Naciones Unidas y el reconocimiento internacional de los derechos individuales, por medio de la Declaración Universal de los Derechos Humanos.
- Tras el fin de la Segunda Guerra Mundial, una cantidad de factores generan el surgimiento de un nuevo conflicto de carácter ideológico, político, tecnológico y militar conocido como Guerra Fría, que marcó la segunda mitad del siglo XX. Como consecuencia de este conflicto el mundo ve nacer una fuerte competencia entre las dos superpotencias (EEUU y URSS) que se traduce en el desarrollo a pasos agigantados de nuevas tecnologías en las más diversas áreas.
- Con el final de la Guerra Fría estas tecnologías son puestas a disposición del público, lo cual culmina con el surgimiento de la actual Sociedad de la Información; la cual se caracteriza por encontrarse las nuevas tecnologías (especialmente las TICs) totalmente inmersas en todas las actividades sociales, culturales y económicas.
- Ante los fenómenos de la sociedad de la información surge también el concepto de *personalidad virtual*, el cual responde a la necesidad de extender sus derechos y deberes al ámbito virtual (o ciberespacio) creado por las nuevas tecnologías.

## Derechos Humanos, Derechos Fundamentales y Derechos de la Personalidad

*A lo largo de la cual se definen las características y se detallan las diferencias existentes entre estos tres conceptos.*

### Derechos Humanos

- Son comprendidos como el conjunto de derechos inherentes a la persona humana por el mero hecho de serlo, por lo que no dependen de su reconocimiento por los Estados para ser atribuibles a todo ser humano.

- Estos derechos se fundamentan en atributos humanos que preceden cualquier garantía y disposición estatal (la dignidad y personalidad del ser humano). Si bien es cierto que se trata de un concepto dinámico, en la actualidad son considerados bienes jurídicos subjetivos exigibles erga omnes.
- Sus principios fundamentales son: universalidad; historicidad; inalienabilidad; positividad; dignidad; permanencia; facultatividad; autonomía; imprescriptibilidad; incondicionalidad; e inviolabilidad.
- Existen múltiples clasificaciones; la más popular de todas es la clasificación *generacional*, la cual los clasifica de la siguiente manera:
    - Derechos de primera generación: Derechos fundamentales inherentes al individuo de naturaleza civil y política.
    - Derechos de segunda generación: Derechos sociales, económicos y culturales, mediante los cuales se demanda un estado de bienestar que garantice el goce de las personas en sociedad.
    - Derechos de tercera generación: Derechos de los pueblos, dirigidos a asegurar la cooperación de estos, con miras asegurar el cumplimiento de intereses colectivos comunes a todas las naciones o grupos.

Derechos Fundamentales

- Pueden ser definidos como aquel conjunto de derechos subjetivos y libertades reconocidos a toda persona (ciudadano o persona) por las normas jurídicas imperantes en cada Estado.
- Se encuentran fundamentados en el reconocimiento que de estos derechos realice el Estado, aunados con el reconocimiento del individuo como ciudadano o persona por parte de dicho Estado; son caracterizados por considerarse indisponibles e inalienables una vez que estos han sido reconocidos a un individuo.
- No pueden ser limitados por disposiciones legales ordinarias en tanto se fundamentan en disposiciones normativas de rango constitucional.
- Cuentan con tres características fundamentales, a saber:

- Su sujeto activo es el gobernado (mientras que en el caso de los derechos humanos el sujeto activo es todo ser humano).
- Su principal sujeto pasivo es el Estado y sus autoridades (lo cual no niega que estos puedan ser protegidos por los sujetos pasivos aún en las relaciones privadas).
- Su fuente máxima puede encontrarse en la Constitución Política de cada país y su finalidad puede ser identificada como *"la protección de la dignidad humana para el pleno desarrollo de la personalidad de las personas físicas, ya sea directamente o indirectamente a través de las personas morales" (De la Parra Trujillo, 2001, pág. 154).*

Derechos de la Personalidad

- Tratados tradicionalmente en el contexto del Derecho Civil, se pueden definir estos derechos como aquellos *"derechos subjetivos previstos por el ordenamiento jurídico positivo que tutelan la dignidad de la persona, a través de la protección de ciertos bienes constituidos por proyecciones físicas o psíquicas del ser humano, atribuidas para sí u otros sujetos de derecho" (De la Parra Trujillo, 2001, pág. 154)*.
- Su principal fundamento es la legislación interna de cada país, por lo que derivan también de los principios establecidos constitucionalmente. A pesar de ello, resulta importante recalcar que a lo largo de su (corta) historia, la protección de estos derechos ha sido abordada de tres maneras diferentes por los diversos Estados, dependiendo de la tesis con la que comulguen sus legisladores:
  - Tesis Monista: Protege un único derecho a la personalidad como unitario y de imposible fraccionamiento.
  - Tesis Pluralista: Procura el establecimiento positivo de cada manifestación de la personalidad digna de protección.
  - Tesis Mixtas: Protegen dentro del sistema jurídico un derecho general a la personalidad, complementado por una pluralidad de derechos relativos a sus manifestaciones específicas.

- A pesar de ser relegados originalmente al ámbito del Derecho Privado, actualmente estos derechos son equiparados, por la mayor parte de los países, con los derechos fundamentales.
- Sus características principales incluyen su carácter como derechos subjetivos; el ser patrimoniales pero no pecuniarios; ser personalísimos; ser variables; absolutos; intransmisibles; irrenunciables; inembargables e imprescriptibles.
- El sistema de clasificación estudiado para estos derechos los divide en:
    - Derecho a la Identidad: Conformado tanto por elementos físicos como dinámicos (identidad, patrimonio cultural).
    - Derechos relativos al cuerpo: Directamente relacionados con la integridad física del individuo (vida, integridad física, libre disposición del cuerpo).
    - Derechos relativos a la identidad moral: Relacionados directamente con los aspectos morales del individuo (libertad, honor, intimidad, privacidad, autodeterminación informativa, imagen y voz).

## Sección II: Intimidad, Privacidad, Información y Autodeterminación Informativa como Bienes Jurídicos Tutelados en el Derecho Nacional e Internacional

Este apartado se dedicará a identificar las características generales de los derechos más relevantes para la protección de datos personales, con miras a dilucidar sus características fundamentales. Para ello se estudiarán, en primera instancia, los derechos a la intimidad y a la privacidad; se detallará el examen de las similitudes y las diferencias encontradas entre sus respectivos marcos contextuales.

En segundo lugar, se revisará tanto el derecho a la información como el derecho a la autodeterminación informativa, con miras a comprender sus principios y sus características generales, lo cual ayudará a enfocar de mejor manera sobre la protección de datos y su cabal comprensión.

### *Derecho a la Intimidad y el "Right to Privacy" Anglosajón*

Usualmente confundidos por la doctrina nacional e internacional, los derechos a la intimidad y a la privacidad responden fundamentalmente a dos contextos legales distintos. Si bien ambos derechos hacen referencia a la protección de ámbitos privados de la personalidad individual frente al escrutinio público, mientras que el derecho a la intimidad ha sido desarrollado por el Derecho Civil de los países europeos y latinoamericanos; el derecho a la privacidad o "*privacy*" es comúnmente identificado como una elaboración del derecho anglosajón.

La rápida evolución de las tecnologías de la información y la comunicación dada en la actualidad, ha sido normalmente identificada como la causa de los acalorados debates llevados a cabo por la doctrina sobre las diferencias y similitudes entre ambos términos. Estos debates, actualmente considerados como superados, impulsaron el avance de la doctrina y permitieron finalmente identificar las bases del derecho a la autodeterminación informativa que actualmente conocemos.

Debido a tal situación, se hace necesario presentar al lector un análisis de lo que nuestro Derecho Civil comprende actualmente como *derecho a la intimidad*; para esto se detallarán las diversas definiciones existentes, sus fundamentos, naturaleza jurídica, características generales, sus elementos constitutivos y finalmente sus manifestaciones en el Derecho positivo tanto nacional como internacional, que lo establecen como un bien jurídico tutelado.

Una vez concluido este análisis, se tratará brevemente el *derecho a la privacidad*, con miras a caracterizar aquellos aspectos que para el derecho anglosajón resultan elementales. Así, se revisarán tanto sus fundamentos y definiciones, como parte de la legislación y jurisprudencia que lo sustentan dentro del *Common Law*[19].

## El Derecho a la Intimidad

Inicialmente ideado como herramienta de protección de la sociedad burguesa contra el *"intervencionismo y arbitrariedad de los poderes públicos" (Bru Cuadrada, 2007),* el derecho a la intimidad se constituye hoy en fundamento mismo de la vida democrática de todo Estado Social de Derecho, por lo cual actualmente resulta innegable su reconocimiento internacional como un derecho humano.

El derecho a la intimidad actual supera los meros conceptos de autonomía, aislamiento y exclusión que caracterizaron su iteración burguesa y es concebido por el Derecho costarricense como un derecho fundamental, que manifiesta la obligación estatal de garantizar el pleno desarrollo de la personalidad y dignidad individual.

### *Fundamentos y Definición del Derecho a la Intimidad*

[19] Se limitará este punto únicamente al estudio de la legislación y jurisprudencia estadounidenses, en tanto resulta más relevante dado nuestro contexto y el fin de la presente investigación.

Según Edward Bloustein, resulta posible identificar los fundamentos del derecho a la intimidad en la libertad y dignidad individual. Conforme a su carácter de derecho humano y derecho fundamental, este derecho tiene como fin la defensa de la dignidad humana y puede ser comprendido como base de la libertad individual existente en los sistemas democráticos modernos *(Morales Godo, Derecho a la Intimidad, 2002, págs. 98, 101).*

El fundamento de este derecho también ha sido analizado por la jurisprudencia constitucional costarricense al establecer que *"En una democracia todo ciudadano tiene derecho a mantener reserva sobre ciertas actividades u opiniones suyas y obtener amparo legal para impedir que sean conocidas por otros…"; resulta imposible o muy difícil convivir y desarrollar a plenitud los fines que una persona se propone sin gozar de un marco de intimidad, protegido de injerencias del Estado u otros ciudadanos" (Hernández Valle, 2008, pág. 86)*.

Morales Godo señala que este derecho ha sufrido una importante evolución histórica, siendo considerado en diversos momentos históricos como: el derecho a la inviolabilidad de la seguridad personal (personalidad inviolada); el *"derecho a ser dejado solo y tranquilo"* o *"a ser dejado en paz"*; el derecho *"de gozar de la existencia sin que su nombre o su vida sean explotados para fines comerciales"*; y como el *"derecho a la felicidad, lo cual incluye estar libre de ataques innecesarios al carácter, al status social o reputación"* (Morales Godo, Instituciones del Derecho Civil, 2009, pág. 276).

De esta manera, por más que la doctrina ha intentado formar una definición de aquello que se entiende como derecho a la intimidad, debe recalcarse que este es un término que varía y se adapta a los diferentes contextos históricos y sociales en que se

ha utilizado; por ello, actualmente se comprende que no existe una definición que enmarque de manera unívoca la totalidad de los usos y posibilidades del concepto.

Según García Fernández, *"la palabra intimidad tiene su origen en el vocablo latino intimus, que significa: zona espiritual reservada de una persona, así como de un grupo o de una sola familia"* (García Fernández, 2002); esta primera aproximación al tema culmina para la autora con la afirmación de que *"Es entonces el derecho a la privacidad o a la intimidad la facultad que tiene un individuo de disponer de un terreno o espacio de su libertad individual, el cual no debe ser invadido por otras personas, sin su consentimiento" (García Fernández, 2002).*

Esta definición concuerda con la posición de Hassemer & Chirino, quienes recuerdan el concepto de intimidad manifestado por Pablo Lucas Verdú, quien se refiere *a lo más recóndito*, relacionándolo con la idea de *sacralidad* en tanto lo íntimo puede ser entendido como algo sagrado, no divulgable sin el consentimiento de aquel sobre quien versa la información *(Hassemer & Chirino, 1997, pág. 89).*

Esta misma línea de pensamiento comparten Ávila Hernández, Castaldo & Urdaneta Meza, quienes consideran que "el derecho a la intimidad protege la parte más íntima de una persona, esto es, esa esfera personal que define qué es y qué no es privado. (…) Se trata en definitiva de aquellos datos que bajo ninguna circunstancia proporcionaría un individuo de manera libre y consciente*" (Ávila Hernández, Castaldo, & Urdaneta Meza, 2007).*

Por su parte, Rojas Vega & Vargas Delgado facilitan varias definiciones del derecho a la intimidad, partiendo de su propia definición, según la cual nos encontramos ante *"Un derecho humano fundamental por virtud del cual se tiene la facultad de excluir o negar a las demás personas del conocimiento de ciertos aspectos de la vida de cada persona, que solo a ésta le incumben" (Rojas Vega & Vargas Delgado, 2009, pág. 179).*

Asimismo, los autores facilitan la definición de Araya Pérez, quien considera que *"El derecho a la intimidad consiste en poder preservar la libertad de la persona en lo íntimo, a la cual se oponen tanto la fiscalización intrusiva como la difusión instrumentalizadora" (el aspecto privado de las personas no puede ser controlado ni observado por otros ni mucho menos puede ser utilizada esta información para fines no autorizados.)" (Rojas Vega & Vargas Delgado, 2009, pág. 180).*

De manera más sucinta, Castañeda Cordy la define como aquel *"derecho personalísimo que permite sustraer a la persona de la publicidad o de otras turbaciones de la vida privada, el cual está limitado por las necesidades sociales y los interesas públicos" (Rojas Vega & Vargas Delgado, 2009, pág. 179).*

Finalmente, dada su amplitud, el suscrito autor de esta investigación se inclina hacia la adopción de la definición brindada por Sánchez Bursón en Rojas Vega & Vargas Delgado, según la cual *"La intimidad es la parte de la vida de una persona que no ha de ser observada desde el exterior, y afecta sólo a la propia persona. Se incluye dentro del ámbito privado de un individuo cualquier información que se refiera a sus datos personales, relaciones, salud, correo, comunicaciones electrónicas privadas, etc. Es el derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida personal, es decir, de sus sentimientos y comportamientos. Una persona tiene el derecho a controlar cuándo y quién accede a diferentes aspectos de su vida personal" (Rojas Vega & Vargas Delgado, 2009, pág. 179).*

### *Naturaleza Jurídica y Características del Derecho a la Intimidad*

A partir de un estudio de la historia del derecho a la intimidad, resulta posible observar fundamentalmente que el tratamiento dado originalmente al concepto, respondía al desarrollo dogmático que clasificaba la tutela brindada al ciudadano por medio de una serie de esferas concéntricas (o *esferas de aislamiento*); la más interior de ellas es comprendida como un espacio del que el individuo es único titular, dentro del cual el sujeto posee la facultad de excluir a otros de sus asuntos (visión patrimonial de la intimidad).

Según Hassemer & Chirino, tal clasificación tuvo como consecuencia la escisión de la esfera íntima del ciudadano de la protección brindada por las esferas subsecuentes, tomándola solamente como *"una expresión de los derechos del ciudadano en algunas facetas de su vida privada" (Hassemer & Chirino, 1997, pág. 91).*

Este *tratamiento incompleto* de la intimidad tuvo como consecuencia la extrema especialización del ámbito original de aplicación del derecho a la intimidad, el cual, a diferencia del "privacy" anglosajón, se encontraba limitado solamente a la visión patrimonial de la intimidad y olvidaba la protección de aspectos relativos a los círculos subsecuentes; que igualmente resultarían relevantes para la protección de la personalidad del individuo en una sociedad cambiante y cada vez más informatizada.

En la actualidad, el derecho a la intimidad ha debido superar las limitaciones representadas por la visión patrimonial de la intimidad, adoptando elementos de protección a elementos de la vida privada y la privacidad[20] de la persona que no necesariamente forman parte de la intimidad individual tradicional.

[20] Se denota de esta manera cierta tendencia hacia la unificación de ambos conceptos.

Según Urabayen *(Herrán Ortiz, 2002)*, el contenido del derecho a la intimidad actual no se encuentra restringido meramente a aquellos aspectos puramente internos del individuo que tradicionalmente han configurado la dimensión *restrictiva* de la intimidad; sino que puede extenderse también a la llamada *vida privada* de la persona, la cual trata de aspectos privados del individuo que no forman parte necesariamente de la intimidad de este.

Esta situación actual puede ser ejemplificada a partir del examen de las definiciones anteriores, en las cuales es posible identificar dos puntos compartidos por todas ellas; a saber: el derecho a la soledad (manifestación de la visión tradicional de la intimidad) y el control de la información (manifestación de las nuevas extensiones adquiridas por la intimidad).

Estas nuevas extensiones de la intimidad, pueden ser entendidas siguiendo el razonamiento de Herrán Ortiz, quien considera que *"el derecho a la intimidad aparece entonces configurado desde una doble perspectiva: una negativa o de exclusión, propia de los derechos subjetivos, y que se traduce en el derecho a excluir intromisiones de terceros en la esfera privada de la persona; y una perspectiva positiva, de control y decisión por el interesado de la disposición sobre la información que le afecta"* (Herrán Ortiz, 2002).

Esta doble perspectiva de la intimidad, refiere a su vez los elementos fundamentales de la Dignidad humana, los cuales son, según Peña Ortíz & Achío Gutiérrez, *"la consideración de que es indispensable dotar a la persona de un derecho a su autodeterminación y por otro lado, un derecho a interactuar en la sociedad como un eje de imputaciones jurídicas"* (Peña Ortiz & Achío Gutiérrez, 2011, pág. 11).

Más aún, esta doble perspectiva dota a la intimidad de una serie de características específicas que responden a su especial condición como derecho subjetivo y bien jurídico tutelado, dentro de las cuales se pueden encontrar las siguientes:

- Abarcan y protegen tanto los ámbitos meramente individuales de la persona como los de su núcleo familiar, "dado que esos vínculos inciden en la esfera de la personalidad de cada uno" (Peña Ortiz & Achío Gutiérrez, 2011, pág. 10).
- Se trata de un derecho personalísimo, no extensible a las personas jurídicas.
- Dota al individuo tanto de medios de defensa procesal (en tanto es un bien jurídico tutelado por el ordenamiento) como de derechos a su disposición (dado su carácter de derecho subjetivo) *(Morales Godo, Derecho a la Intimidad, 2002, pág. 104).*
- Su protección recae tanto en el individuo como en el Estado; debe encargarse este último de velar por su correcta aplicación, tanto por parte de entes privados como por parte de entes públicos.
- Garantiza un ámbito privado "*reservado a la propia persona y del que quedan excluidos los demás, salvo, desde luego, que el titular del derecho desee compartir esa zona de privacidad con otros semejantes" (Hernández Valle, 2008, pág. 86)*.
- Es un fundamento del derecho a la autodeterminación informativa en tanto comprende la potestad individual de controlar que un tercero conozca o no nuestra vida privada y la posibilidad de controlar lo que otros conocen de nosotros *(Bru Cuadrada, 2007, pág. 81)*.

- Al igual que los otros derechos de la personalidad, es irrenunciable, imprescriptible, inalienable, intransmisible e inembargable *(Bru Cuadrada, 2007, pág. 81)*.

### *Elementos del Derecho a la Intimidad*

El derecho a la intimidad comprende diversos elementos, dentro de los cuales usualmente se encuentran los siguientes (Rojas Vega & Vargas Delgado, 2009):

- Derecho a la Inviolabilidad del domicilio
- Derecho a la inviolabilidad de la correspondencia y las comunicaciones
- Derecho a la propia imagen
- Derecho al honor
- Derecho a no participar en la vida colectiva y al aislamiento voluntario
- Derecho a la privacidad informática

Cada uno de estos elementos del derecho a la intimidad ha sido tratado de manera diversa por la doctrina, la cual les ha dado diversos niveles de importancia según la percepción que cada autor tenga de estos derechos y de la esfera de aislamiento a la cual asigne cada elemento.

Según la doctrina italiana, las esferas de aislamiento que usualmente pueden ser distinguidas son las siguientes:

> *"1) La soledad, que entraña la imposibilidad física de contactos materiales;*

*2) La intimidad, en la que el individuo, sin hallarse aislado, se encuadra en un grupo reducido en el que se dan relaciones especiales, como por ejemplo en el ámbito conyugal y familiar;*

*3) El anonimato;*

*4) La reserva, que consiste en la creación de una barrera psicológica frente a las intromisiones no deseadas" (Pfeffer Urquiaga, 2000, pág. 466).*

La actual concepción "amplia" del derecho a la Intimidad busca superar estas esferas por medio de la admisión de tres elementos básicos que determinan la protección brindada por este derecho al individuo. Estos tres elementos constituyen el ámbito privado protegido por el derecho a la intimidad y son protegidos tanto en forma negativa como positivamente por el individuo.

A partir del estudio de las obras de Rojas Vega & Vargas Delgado y Peña Ortíz & Achío Gutiérrez, se pueden identificar estos elementos fundamentales del derecho a la intimidad como: la vida privada, la privacidad y la autonomía de la voluntad.

*Vida Privada*

Morales Godo, en su obra *Derecho a la Intimidad*, señala que, al igual que con respecto al concepto de intimidad, no existen en la actualidad criterios uniformes sobre lo que se llama *vida privada*; debido a que tal concepción varía según cambian las tradiciones, las culturas e incluso las generaciones.

A pesar de tal realidad, la doctrina no ha cesado en sus esfuerzos por definir el concepto de *vida privada*. Dada la relevancia que dicho concepto presenta para la legislación costarricense, a continuación se hará referencia a algunos de estos esfuerzos.

La primera de las definiciones encontradas la brinda Rivero, quien es citado en Peña Ortiz & Achío Gutiérrez, y en la cual manifiesta que *"la vida privada es aquella esfera de cada existencia en la cual nadie se puede inmiscuir sin haber sido autorizado. La libertad en la vida privada es el reconocimiento en beneficio de cada uno, de una zona de actividad que le es propia, en que se es dueño de prohibir a los demás"* (Peña Ortiz & Achío Gutiérrez, 2011, pág. 11).

Araya Pérez, citado por Rojas Vega & Vargas Delgado, considera que *"la vida privada es la vida familiar, personal, su vida interior, la que lleva cuando vive detrás de su puerta cerrada... se dice también que es el conjunto de modos de ser y vivir, de estados afectivos, de acciones y reacciones que se desarrollan en el hogar, y no tienen por qué trascender a la vida social pública de una colectividad...dentro de la misma idea, vida privada se define como aquellos datos hechos o situaciones desconocidas para la comunidad, que son verídicos, y que están reservados al conocimiento, bien del sujeto mismo, bien de un grupo reducido de personas, cuya divulgación o conocimiento por otros trae aparejado algún daño patrimonial o moral"* (Rojas Vega & Vargas Delgado, 2009, pág. 182).

Por su parte, Hernández Valle considera que *"La vida privada comprende, ante todo, la vida interior y luego toda aquella parte de la vida exterior que no se considera parte del ámbito público. En otros términos, la vida privada del hombre moderno abarca hasta donde se extiende su libertad y no se restringe únicamente al dominio interno de su conciencia, o de la persona física o al inmediato ambiente actual o habitual del individuo, ya que esta libertad se*

*manifiesta en otro campo vastísimo que se encuentra más allá de cualquier control político directo: el mundo de la cultura"* (Hernández Valle, 2008, pág. 86).

### *Privacidad*

Comprendida en la actualidad dentro del nuevo ámbito de aplicación del derecho a la intimidad, la privacidad constituye una gama compleja de situaciones que en nuestro derecho son inspiradas a partir del "privacy" anglosajón, al cual busca emular con miras a brindar respuesta efectiva a las técnicas de recopilación masiva de datos personales facilitadas por el avance de las ciencias de la computación.

Parafraseando a Rojas Vega & Vargas Delgado, el concepto de *privacidad* posee un significado más amplio que el de *intimidad* y hace referencia fundamentalmente a todas aquellas informaciones referentes al individuo que, analizadas de manera separada parecieran ser irrelevantes, pero que en conjunto permiten la construcción de perfiles individuales sumamente exactos *(Rojas Vega & Vargas Delgado, 2009, pág. 183).*

Según Peña Ortiz & Achío Gutiérrez, nuestra Sala Constitucional desprende la privacidad del derecho a la intimidad al establecer, en su voto 1026-94 que es *"un fuero de protección a la vida privada de los ciudadanos"* y al preguntarse en su voto 8116-2007 si resulta factible incluir la protección de la información dentro de la esfera privada, *"la cual comprende, no se reduce al domicilio o a las comunicaciones"* (Peña Ortiz & Achío Gutiérrez, 2011, pág. 20).

*Autonomía de la Voluntad*

Olivier Soro Russel, en la introducción a su tesis doctoral titulada *"El principio de la autonomía de la voluntad privada en la contratación"* desgrana las tres palabras ("autonomía", "voluntad" y "privada") que constituyen este principio del derecho y recuerda la importancia de este en el ordenamiento jurídico privado.

La palabra "autonomía", recuerda el autor, *"proviene de la unión de dos términos griegos. Por un lado se encuentra el término nomos, que quiere decir "ley"*. Por el otro, el vocablo o prefijo *autos*, que para la Real Academia Española significa *"propio o por uno mismo""* con lo cual el autor concluye, junto con Laguna, que este término hace referencia al *"poder de dictarse uno a sí mismo su propia ley"* (Soro Russell, 2007, pág. 9).

En segundo lugar, el autor recuerda que la palabra *"voluntad*" atesora un sentido inmenso. Este término, heredero directo de la *voluntas* romana, "es definido en la primera de sus acepciones por la Real Academia como *"Facultad de decidir y ordenar la propia conducta"*. Pero voluntad es también "Libre albedrío o libre determinación" y *"Elección de algo sin precepto o impulso externo que a ello obligue"*. Esto permite al autor entender la voluntad como *"la capacidad de decidir y ordenar la propia conducta sin ser obligado a ello por algún impulso externo"* (Soro Russell, 2007, págs. 9-10).

Por último, se detiene el autor en el adjetivo "*privada",* el cual identifica como *"uno de los elementos en torno al cual gira el conjunto del Derecho común"* y que define como lo

*"particular y propio de cada persona"* y como aquello que se configura en oposición a lo público (Soro Russell, 2007, pág. 10).

A partir de estas tres definiciones conceptuales, el autor establece la definición que puede considerarse como más acertada, en relación con el principio de autonomía de la voluntad, a saber:

*"(…) autonomía de la voluntad privada es la facultad de los particulares para regir y ordenar su propia conducta mediante sus propias normas sin depender de nadie ni ser obligado a ello por algún impulso externo"* (Soro Russell, 2007, pág. 10).

Las características fundamentales de esta definición son compartidas por autores como Spota, quien considera que *"es el principio que confiere a la voluntad jurídica la atribución de crear negocios jurídicos sin ultrapasar el ordenamiento coactivo, brindándoles su contenido y su eficacia jurídica"* (Peña Ortiz & Achío Gutiérrez, 2011, pág. 21); Colin y Capitant, quienes aseguran que *"la autonomía de la voluntad permite a los particulares la ejecución de actos jurídicos con aquellas consecuencias jurídicas que convengan con ciertas limitaciones"* (Pinedo Aubián, pág. 2); y Diez Picazo y Gullón, quienes la señalan como *"el poder de dictarse a uno mismo la ley o el precepto, el poder de gobernarse a uno mismo (…) puede igualmente conceptuarse como el poder de la persona para reglamentar y ordenar las relaciones jurídicas en las que se es o ha de ser parte. La autonomía privada es libertad individual"* (Pinedo Aubián, pág. 2).

A pesar de poseer como elemento fundamental la exclusión de injerencias externas en la formación de la voluntad del individuo, debe recordarse también que el ámbito del principio de autonomía de la voluntad no es ilimitado. En nuestro sistema jurídico, los límites de este principio se encuentran establecidos por el artículo 28 de nuestra

Constitución Política, el cual reza que *"(…) las acciones privadas que no dañen la moral o el orden público o que no perjudiquen a tercero, están fuera de la acción de la ley".*

Los límites establecidos por el artículo constitucional supracitado son estudiados por nuestra Sala Constitucional en su Resolución 7494-97. Esta resolución ha sido analizada por Peña Ortiz & Achío Gutiérrez, quienes señalan como fundamental el que considere al ejercicio de la libertad como potencialmente sometido a restricciones y límites, tanto materiales como jurídicos*;* apuntan que esta resolución concluye señalando que

*"la libertad de cada quien termina donde empieza la del otro, y es allí donde el Estado debe intervenir para evitar abusos"* (Peña Ortiz & Achío Gutiérrez, 2011, pág. 21).

De esta manera, puede concluirse que en el sentido actual, la autonomía de la voluntad es considerada uno de los principios rectores del hombre, fundamento de la libertad individual, cuyo carácter dinámico posee límites claros, los cuales son plasmados en la máxima de John Stuart Mill, la cual rezaba que: *"la única libertad que merece ese nombre es la de buscar nuestro bien por nuestro propio camino en tanto no privemos a los demás del suyo" - John Stuart Mill.*

### *Distinción entre lo Público y lo Privado*

Tal como se estudió con anterioridad, de conformidad con las teorías tradicionales, la intimidad puede ser comprendida como el círculo más "reservado" de protección en las relaciones entre el individuo y la sociedad. Para la corriente doctrinaria que estudia

de esta manera la intimidad, un punto álgido siempre ha podido ser identificado en la necesidad de establecer algún límite entre lo público y lo privado.

De acuerdo con Morales Godo y Pfeffer Urquiaga, resulta imposible establecer, de manera universal, una distinción precisa entre lo público y lo privado. Tal límite ha sido reiteradamente tratado tanto por la jurisprudencia como por la doctrina, sin que ello se viera traducido en acuerdo.

El Profesor Emilio Pfeffer Urquiaga, en su artículo *"Los derechos a la intimidad o privacidad, a la honra y a la propia imagen. Su protección frente a la libertad de opinión e información",* intenta brindar al lector una breve introducción a las diversas maneras en que tal límite ha intentado determinarse; algunas de las cuales son:

- A partir de la calidad de la persona (un sujeto público, ejerciendo una función pública o con algún tipo de notoriedad, ha de contar con un ámbito de vida privada más limitado que el de la persona promedio).
- A partir del espacio en el que suceden los hechos (un hecho sucedido en un espacio recluido, tal como una vivienda podría ser comprendido como privado).
- A partir de la titularidad de las necesidades satisfechas por el acto (si se satisface una necesidad ajena, podría comprenderse el acto como público).
- A partir del conocimiento de los hechos (si son desconocidos para terceros y el sujeto desea que tal situación se mantenga, se consideran privados) (Pfeffer Urquiaga, 2000, pág. 467).

Por su parte, el tratadista Eduardo Novoa Monreal, citado por Peña Ortiz & Achío Gutiérrez, considera como elementos esenciales para tal diferenciación los siguientes: *"a) Que los hechos sean desconocidos.*

*b) Que los hechos sean de aquellos que la persona desea mantener reservados.*

*c) Que los hechos sean susceptibles de producir turbación moral, molestia o intranquilidad, en caso de que el mismo fuera revelado o conocido por alguien.*

*d) La violación debe ser arbitraria, sin derecho o causa justa" (Peña Ortiz & Achío Gutiérrez, 2011).*

A pesar de tales esfuerzos, actualmente la doctrina ha llegado a considerar (acertadamente en opinión del suscrito autor de esta investigación), que cualquier esfuerzo de distinción entre los ámbitos públicos y privados, solamente puede establecerse a partir de la interpretación jurisprudencial (Morales Godo, Derecho a la Intimidad, 2002, pág. 108) que determine de manera casuística cuáles hechos corresponden a la vida pública o privada.

### *Limitaciones del Derecho a la Intimidad*

Tal como sucede en el caso del principio de autonomía de la voluntad, el derecho a la intimidad no es absoluto, y su protección se encuentra basada en un justo equilibrio de los intereses individuales y generales. Así, nuestra Sala Constitucional en su voto número 678-91 consideró que *"tratándose de la libertad e intimidad de los ciudadanos, el constituyente les garantizó un ámbito propio, su esfera privada, que en principio es inviolable y*

*solo parcialmente allanable con intervención del Juez en procura de resguardar bienes jurídicos de mayor jerarquía"* (Sala Constitucional de la Corte Suprema de Justicia, 1991).

Estos bienes jurídicos de mayor jerarquía son usualmente aquellos considerados "de interés público", los cuales son entendidos por Morales Godo como aquellas situaciones en las cuales *"el acto o el hecho tiene trascendencia social" (Morales Godo, Instituciones del Derecho Civil, 2009, pág. 278)*.

Así, existen ejemplos de límites al derecho a la intimidad en aquellos casos en los que un juez determine la existencia de razones que aseguren de manera indudable, que la limitación de la intimidad individual será ejercida en protección de la seguridad nacional, el bien común, el orden y seguridad pública, la salud o la moralidad pública o en caso de que se vean afectados derechos o libertades individuales de manera directa y sea necesario protegerlos de tales afectaciones.

## *Manifestaciones del Derecho a la Intimidad en el Derecho Nacional e Internacional*

### *La Intimidad como Bien Jurídico Tutelado en el Ámbito Nacional*

Tal como lo ha sido estudiado, el derecho a la intimidad personal ya no es solamente comprendido como un derecho de la personalidad, sino que en la actualidad es considerado como un derecho humano protegido y garantizado tanto en el ámbito nacional como en el internacional, por medio de diversos estatutos normativos que

buscan la tutela de sus titulares y la garantía de su pleno ejercicio en los diversos ámbitos legales.

Por su parte, el Derecho costarricense ha adoptado esta percepción del derecho fundamental a la intimidad como derecho irrenunciable, que se encuentra basado en la dignidad humana y que es a su vez fundamento de la democracia y de la libertad individual. En el Derecho positivo nacional, existe fundamento al derecho a la intimidad en el texto constitucional mismo. En el artículo 33 constitucional se procura la defensa de la dignidad humana y el artículo 24 establece expresamente el deber de garantizar el derecho a la intimidad, a la libertad y al secreto de las comunicaciones, para a continuación establecer las condiciones en que deberá llevarse a cabo tal protección y las condiciones en las cuales podrán establecerse límites legales a tales derechos.

A partir de estos fundamentos, nuestra jurisprudencia constitucional ha reconocido a este derecho con una doble connotación, tanto de interés particular como social, con un ámbito de aplicación que supera la esfera de lo más íntimo del ser humano y se manifiesta también en las esferas exteriores, las cuales contemplan la información que sobre el individuo manejan terceros (incluyendo al Estado).

De esta manera, es de especial relevancia para el tema recordar que nuestra Sala Constitucional ha manifestado en sus votos 1261-90, 5736-94 y 8022-99 que *"el derecho a la intimidad es entre otras cosas el derecho del individuo a tener un sector personal, una esfera privada de su vida, inaccesible al público salvo expresa voluntad del interesado, el cual está contenido en forma expresa en el artículo 24 de la Constitución Política",* y en su sentencia 1261-90, afirmó que los ciudadanos tienen el derecho *"…a mantener reserva*

*sobre ciertas actividades u opiniones suyas y obtener amparo legal para impedir que sean conocidas por otros, en especial cuando para reconocerlas deban emplearse procedimientos clandestinos; resulta imposible o muy difícil convivir y desarrollarse a plenitud, sin estar protegido de injerencias del Estado y otros ciudadanos".*

En tanto esta protección de injerencias del Estado y otros ciudadanos adquiere cada día mayor relevancia, conviene recordar las palabras de Hassemer & Chirino, quienes consideran acertadamente que:

*"Hoy en día esta "patrimonialización" que refiere la tutela de la intimidad a la concentración en "bienes personalísimos" del sujeto como los "secretos" y el "honor" (área de la privacy como esfera íntima), se amplía con una tutela del habeas mentem del ciudadano. En este contexto, se entiende que la libertad de los ciudadanos y su garantía ya no proviene exclusivamente del derecho privado, sino que adquiere connotaciones constitucionales que la unen de manera inescindible a valores tales como la dignidad humana y el desarrollo de la personalidad"* (Hassemer & Chirino, 1997, pág. 93).

En un contexto en el que el derecho a la intimidad supera la protección del Derecho Privado y es contemplado y protegido por las diversas esferas públicas, son trascendidas las dificultades que supone para el ciudadano la protección efectiva de su derecho a la intimidad, en un mundo cada vez más interconectado. Es en esta protección mixta a la intimidad contemplada por nuestro ordenamiento jurídico donde encontramos el verdadero carácter de este derecho como bien jurídico tutelado.

En el ámbito internacional, existen referencias al derecho a la intimidad en diversos convenios internacionales, los cuales, al ser ratificados por cada país, deben ser

integrados dentro de su marco regulatorio aplicable. A continuación se procederá a la revisión de algunos de estos instrumentos.

*Manifestaciones del Derecho a la Intimidad en el Plano Internacional*

Declaración Universal de Derechos Humanos.

La Declaración Universal de Derechos Humanos, documento declarativo adoptado por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948 en París, recoge los derechos humanos considerados básicos a lo largo de su articulado, dentro del cual se hace mención a la intimidad en el artículo 12, el cual dispone que:

*"Artículo 12 - Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Organización de las Naciones Unidas, 1948).*

Debe resaltarse que según Riascos Gómez, la protección brindada por este artículo responde a una visión de la intimidad desde el derecho anglosajón (Privacy) y se caracteriza por incluir tanto la intimidad personal tradicionalmente entendida como también la *"institución socio-jurídica de la familia", "la intimidad primigeniamente epistolar (escrita)"* (Riascos Gómez, 1999, pág. 54) y culmina por reforzar la percepción del hogar

como centro inexpugnable de derecho a la intimidad personal, que responde al viejo adagio anglosajón el cual reza *"my home is my castle"* (mi casa es mi castillo).

### Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales

Adoptado por el Consejo de Europa el 4 de Noviembre de 1950, el Convenio Europeo de Derechos Humanos se inspira en la Declaración Universal de Derechos Humanos; muestra en relación con este solamente algunas diferencias puntuales (Riascos Gómez, 1999, pág. 58). Posee la característica fundamental de ser vinculante para los países miembros de la Unión Europea, por lo que permite el control judicial del respeto a los derechos individuales.

En lo relevante a la protección de la intimidad, el convenio establece en su artículo octavo que *"toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o la moral, o la protección de los derechos y las libertades de los demás"* (Consejo de Europa, 1950).

El estudio de este artículo pone en evidencia su importancia, al establecer el carácter de derecho fundamental y autónomo de la intimidad y de la vida privada y familiar. Según Riascos Gómez, esta caracterización del derecho implica que puede ser limitado

o su ejercicio restringido, siempre y cuando tal límite se fundamente en causales expresamente previstas y sin que nunca se pueda llegar a desvirtuar los derechos, a hacer nugatorio su ejercicio o a eliminarlos (Riascos Gómez, 1999, pág. 58).

### Pacto Internacional de Derechos Económicos, Sociales y Culturales

El Pacto Internacional de Derechos Económicos, Sociales y Culturales es un tratado multilateral adoptado por la Asamblea General de las Naciones Unidas mediante Resolución 2200A (XXI) del 16 de diciembre de 1966 que a la fecha ha sido ratificado por 160 países.

Este tratado *"reconoce el fundamento socio-jurídico y los elementos del derecho a la intimidad, así como la obligación del Estado y los mismos particulares de su respeto y protección" (Riascos Gómez, 1999, pág. 60).* Esto sin que se llegue a hacer mención explícita a la vida privada, pero reconociendo que este derecho se desprende de la dignidad inherente a la persona humana y caracterizando sus elementos en sus artículos 10, 11, 12 y 13; en ellos se reconoce el derecho al nivel de vida adecuado y el libre consentimiento, a la familia, a la salud física y mental, a la educación tendiente al pleno desarrollo de la personalidad humana y del sentido de su dignidad y el derecho a la vida cultural y al progreso científico (Organización de las Naciones Unidas, 1966).

### Pacto Internacional de Derechos Civiles y Políticos

Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de las Naciones Unidas en su resolución 2200 A (XXI) del 16 de diciembre de 1966, este tratado internacional (mejor conocido como *Pacto de New York*) busca el establecimiento de mecanismos de protección y garantía de los derechos civiles y políticos, para lo cual trabaja en conjunto con el Pacto Internacional de Derechos Económicos, Sociales y Culturales.

A lo largo de su preámbulo, este tratado reconoce la dignidad inherente a la persona humana y en su artículo 17 busca la protección de la persona frente a "injerencias arbitrarias o ilegales contra su vida privada, familia, domicilio, correspondencia, honra y reputación" (Organización de las Naciones Unidas, 1966); lo cual, según Fariñas (citado por Riascos Gómez) es realizado de manera textual casi idéntico al artículo 12 de la Declaración Universal.

A pesar de su similitud, afirma Riascos Gómez que este artículo se encuentra inmerso en un marco jurídico totalmente diferente al de la Declaración al correlacionar a la intimidad otros derechos *"que influyen directa o indirectamente en su constitución"* (Riascos Gómez, 1999, pág. 61).

### Convención Americana sobre Derechos Humanos

Suscrita en la Conferencia Especializada Interamericana de Derechos Humanos el 22 de noviembre de 1969, en la ciudad de San José, Costa Rica (por lo que es también conocida como *Pacto de San José*), la Convención se constituye como una de las bases

del sistema interamericano al reconocer los Estados partes su deber de garantizar los derechos y libertades establecidos por dicha convención en sus propios sistemas legislativos de manera obligatoria, en caso de no poseer ya disposiciones al respecto.

Sobre el derecho a la intimidad, la Convención establece en su artículo 11 que *nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra injerencias o esos ataques* (Organización de los Estados Americanos, 1969).

Según Riascos Gómez, el pacto busca profundizar en la protección del derecho a la intimidad por medio de la protección de dos aspectos nucleares al derecho: la honra y la dignidad humana. A la vez reconoce en su artículo 13 el derecho a la libertad de expresión, estableciéndose que este derecho "observará el respeto (límite jurídico a otro derecho) del derecho a la intimidad (art. 13-2ª)", a la vez que, según el autor, se reconoce el derecho a rectificación y respuesta, y corrobora la autonomía y la correlación de la existencia de estos derechos con el derecho de autodeterminación informativa (Riascos Gómez, 1999, pág. 66).

## El Derecho a la Privacidad (el "Right to Privacy" Anglosajón)

Tal como se estableció con anterioridad, a pesar de hacer referencia a la protección de ámbitos privados de la personalidad individual, se entenderá a lo largo de la presente

investigación que el derecho a la privacidad (o *right to privacy*) es una creación del derecho anglosajón, por lo cual responde a un contexto legal distinto de aquel que genera nuestro derecho a la intimidad (Derecho Civil o Continental).

A pesar de sus diversos contextos, en nuestro país, al igual que en la mayor parte de los países de habla hispana, la separación entre uno y otro derecho se ha visto afectada fundamentalmente por la íntima relación cultural generada en el contexto global de las telecomunicaciones convergentes, la cual ha causado una gran confusión terminológica que ha llegado incluso a verse marcada en el Derecho positivo de nuestros países.

Ante tal situación, a continuación se realizará una breve exploración y caracterización de los fundamentos del derecho a la privacidad, con miras a aclarar al lector las diferencias existentes entre este derecho y el derecho a la intimidad. Para ello se habrá de enfocar el estudio al examen del derecho estadounidense (dada su intensa relación con el presente tema de estudio) y específicamente se habrán de examinar brevemente tanto aquellos fundamentos jurisprudenciales que lo han caracterizado, como su situación en el marco de Derecho positivo vigente actualmente en Estados Unidos.

### *Fundamentos del Derecho a la Privacidad.*

Proveniente del latín "*privatus",* que significa "*separado del resto",* el derecho a la privacidad encuentra sus orígenes, desde la perspectiva del derecho anglosajón, en la publicación del artículo *"The Right to Privacy"* publicado por los autores

estadounidenses Samuel D. Warren y Louis D. Brandeis. Los autores realizan una exploración de dicho derecho a partir de las exposiciones iniciales que sobre el tema realizara el juez Thomas Cooly, quien a su vez identificó este derecho sobre la base del derecho a la propiedad (Rojas Vega & Vargas Delgado, 2009).

A lo largo de su artículo, Warren y Brandeis recorren la evolución de los derechos a la vida, libertad y propiedad, reconociendo la posibilidad de poseer bienes intangibles y cuestionando la aplicación tradicional del derecho a la privacidad por el sistema judicial estadounidense.

Más adelante, critican los autores el vacío legal existente en la época sobre la protección al daño moral causado por la publicación de chismes en los periódicos y continúan desarrollando el derecho a la privacidad de los escritos, vinculando el derecho a la propiedad a la intimidad y señalando algunas de las limitaciones del derecho a la privacidad.

El derecho a la privacidad es concebido de una manera muy diferente a nuestro derecho a la intimidad. Si bien ambos comparten su fin de proteger la esencia moral de la persona, se diferencian en tanto el derecho a la privacidad ha sido entendido por el derecho anglosajón desde sus inicios como una herramienta amplia que soporta el *"right to be left alone"* y ampara también a aquellos elementos de la personalidad que tradicionalmente superan la esfera "*más cercana al individuo*" que caracteriza a nuestro tradicionalmente limitado derecho a la Intimidad.

De conformidad con esta última afirmación existen múltiples definiciones de este derecho, dentro de las cuales se encuentran las siguientes:

*"El derecho a la privacidad es nuestro derecho a mantener un dominio alrededor de nosotros, el cual incluye todas aquellas cosas que son parte de nosotros, tales como nuestro cuerpo, casa, propiedad, pensamientos, secretos e identidad. El derecho a la privacidad nos brinda la habilidad de elegir cuales partes de este dominio pueden ser accedidas por otros, y a controlar la extensión, forma y tiempo en que aquellas partes que elegimos revelar son utilizadas"* (Onn, 2005).[21]

*"(…) la Privacidad es usualmente comprendida como el derecho a vivir en paz, sustrayéndose de la intervención de los terceros en cierto sector de nuestra existencia"* (Domínguez Guillén, 2003).

*"La privacidad es un término más amplio: se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por sí misma puede no ser relevante, pero que analizada en un momento o contexto concretos puede llevarnos a la construcción de un perfil muy fiable del individuo que permita su caracterización e identificación"* (Battaner, 2006).

### *El "Right to Privacy" en Estados Unidos de América*

Según Puente de la Mora, el desarrollo de este derecho en el *Common Law* anglosajón resulta sumamente amplio y se diversifica desde sus orígenes con miras a proteger sus diversos alcances. Así, según la autora, el concepto de *Privacy* responde a *"un tejido interrelacionado de ilícitos civiles (tort law), derecho constitucional federal, derecho*

[21] Esta definición se complementa las ideas de Westin, quien afirmara que "Todo individuo se encuentra continuamente involucrado en un proceso de ajuste personal en el cual él balanza el deseo por privacidad con el deseo de revelación y comunicación de sí mismo a otros, frente a las condiciones ambientales y las normas sociales establecidas por la sociedad en la cual vive" (Westin, 1967).

*constitucional estatal, derecho codificado federal y estatal, información privilegiada, derecho de la propiedad, derecho contractual y derecho penal (criminal law)"* (Puente de la Mora, 2007, pág. 2).

A pesar de la amplitud del tema, a continuación se señalarán algunos de los aspectos fundamentales de este *tejido interrelacionado* con miras a brindar al lector una mejor comprensión.

### *Tratamiento Jurisprudencial en el Common Law*

Para el derecho de los ilícitos civiles del derecho anglosajón, el tema de la privacidad fue marcado desde la década de 1960 por la clasificación realizada por el decano de la Facultad de Leyes de la Universidad de California en Berkeley, William L. Prosser. Esta clasificación es reconocida por autores como Puente de la Mora, Morales Godo y Fernández de Zubiría, como uno de los análisis más importantes existentes sobre el derecho de privacidad anglosajón con los que se cuenta en la actualidad y divide los ilícitos civiles concernientes a la privacidad en cuatro clases fundamentales, a saber:

#### Actos de intrusión que perturban el retiro o soledad del individuo

Se trata de ilícitos que afectan la voluntad del individuo de permanecer "aislado respecto a sus asuntos o relaciones personales" (Puente de la Mora, 2007, pág. 5) que constituye el *right to be let alone* desarrollado por el juez norteamericano Thomas

Cooley. Al respecto de este tipo de ilícitos, Morales Godo señala algunos de sus elementos (intromisiones, fisgoneo y persecución que turba la vida) en los siguientes casos:

a) **Mc Daniel vs. Atlanta Coca Cola Bottling (60 Giorgia App. 92 2d.810. 1939)**; en el que se analiza *"la abierta, pública y persistente persecución de una persona, sin ninguna discreción ni secreto y de manera que se hace evidente al público que ella es perseguida y observada"* por parte de la empresa Coca Cola con miras a forzar a un individuo a saldar sus deudas *(Morales Godo, 2009, pág. 261)*.
b) **Parrish VS. Civil Service Comission (66 California 2d- 260. 1970)**; en el que se declara inconstitucional el chequeo forzoso de las camas de los indigentes de un hogar parte de la Oficina de Bienestar Público de California por considerarse que este chequeo ofendía a la intimidad y dignidad humanas *(Morales Godo, 2009, pág. 262).*
c) **Schultz vs. Frankfurt (130 Wisconsin. 2d.179. 1914);** en el que se califica la conducta de la Compañía de Seguros Frankfurt Company como "libelosa y ofensiva", al demostrarse que *"mediante el uso de detectives y maquinaciones"* intentó forzar a un testigo a mudarse con miras a que no declarara en su contra *(Morales Godo, 2009, pág. 263).*

### Divulgación pública de hechos privados embarazosos sobre el individuo

Posibilita al individuo el establecer una acción contra aquel que publique hechos *altamente ofensivos para una persona razonable y que no sean legítimamente*

*concernientes al público (Puente de la Mora, 2007, pág. 5)* y que ha sido desarrollado en los siguientes casos:

a) **Melvin vs. Reid (112 California appelations. 285 - 1931)**; en el cual el juez establece que *"El derecho a lograr la felicidad está garantizado por la ley fundamental del estado de California. Éste por su propia naturaleza incluye el derecho a vivir libre de ataques de otros en el disfrute de nuestra libertad, propiedad y reputación. Cualquier persona viviendo una vida recta tiene el derecho a la felicidad, lo cual incluye estar libre de ataques innecesarios al carácter, el status social o la reputación"* (Morales Godo, 2009, pág. 265) y contribuyó a aclarar que el *right of privacy* no existe cuando la persona renuncia a sus derechos a la vida privada o cuando se torna *prominente en su vida pública.*

b) **Douglas vs. Stockes (149 Kentucky 506-149 - 1912)**; en el cual un fotógrafo publica fotografías de los rayos x de dos mellizos siameses y el padre de estos reclama indemnización, a lo cual el tribunal da razón considerando que *"los más tiernos afectos del corazón humano están encerrados en el cuerpo de un niño muerto"* como base para permitir la indemnización de *"injurias corporales que pueden causar muchos más sufrimientos y humillación"* como lo son las afectaciones morales (Morales Godo, 2009, pág. 266).

c) **Hemingway vs. Randon Hous (29 appelations Div. 2d. 6333-1968, confirmado en 23 New world 2d. 341 – 1968)**; en el que la esposa del famoso escritor Ernest Hemingway pretende evitar la publicación de la obra *Papa Hemingway*, en la que son transcritas citas exactas de su esposo obtenidas mediante grabaciones magnetofónicas y cartas, por considerarla violatoria a su derecho a la intimidad. El Tribunal de Apelaciones no da razón a la viuda pues considera,

que se encuentra ante una figura pública no protegida por el derecho aludido (Morales Godo, 2009, pág. 267).

### Publicidad que coloca al individuo bajo una luz falsa ante el público

Ilícito que permite la acción cuando la publicidad hace falsas y ofensivas revelaciones respecto a hechos personales (Puente de la Mora, Privacidad de la información personal y su protección legal en Estados Unidos, 2007, pág. 5), especialmente cuando tales hechos sugieren relación directa o indirecta del individuo con alguna opinión o afirmación que no tiene relación alguna con este. Morales Godo señala dos casos que lo ejemplifican fielmente, a saber:

a) **Pinkerton National Detective Agency vs. James A. Stevens (32) (162 South Dakota. 2d. 474 - 1964)**; en el que debido a la vigilancia continua establecida por detectives pagos por una compañía de seguros contra una señora de Dakota, sus vecinos pensaron erróneamente que esta había cometido un delito, lo cual afectó su reputación y es reconocido de esa forma por el tribunal al condenar a la compañía (Morales Godo, 2009, pág. 269).
b) **Lyman vs. New England Newspaper (286 Massachusetts 258-190 NL 542 - 1934)**; en el que a raíz de una publicación en un diario sobre la supuesta infelicidad conyugal de una pareja, el Tribunal condena al pago de una indemnización por violación al derecho a la intimidad de los demandantes al colocárseles *"bajo una luz falsa ante el público" (Morales Godo, 2009, pág. 270).*

Apropiación de la imagen o identidad de una persona para derivar algún beneficio

Ilícito que da a lugar a la protección de la persona ante el uso ilegítimo de su imagen o identidad para fines comerciales, según ha sido tratado en los siguientes casos:

a) **Donohue vs. Wárner Brothers Pictures Inc. (194 Florida 2d.6-10 - 1970)**; en el que el tribunal afirma la existencia del derecho de todo individuo de *"gozar de la existencia sin que su nombre o su vida sean explotados para fines comerciales o con el uso de su nombre o por la publicación de su retrato o carrera, en la pantalla de los cines, en la prensa, en periódicos, en boletines, circulares, catálogos o de cualquier otra manera"* el cual debe protegerse y solamente permitirse su afectación con el consentimiento del interesado (Morales Godo, 2009, pág. 270).
b) **Daily Times Democrat vs. Graham (13 Colorado 2d. 119 - 1963)**; caso característico por basarse en una fotografía tomada a una joven durante su visita a un parque de diversiones en el preciso momento en que una ráfaga de viento levantaba su falda; el tribunal considera que *"aún en lugares públicos hay ciertas cosas que aunque estén a la vista siguen siendo privadas" (Morales Godo, 2009, pág. 271).*
c) **Young vs. Geneker Studies Inc. (175 Misc. 1027 NewYork State 2d. 557 – 1951)**; en el que una modelo demanda a una compañía de ropas infantiles por fabricar y vender sin su consentimiento maniquíes hechos a su medida y forma a terceros, pese a que ella solamente había accedido al uso de tales maniquíes dentro de la tienda. Ante este razonamiento, el tribunal dio razón a la actora y afirma que el consentimiento inicial no restringe su capacidad de invocar

posteriormente su derecho a la intimidad, para protegerse de quien le afectare contra su voluntad (Morales Godo, 2009, pág. 271).

*Derecho Constitucional*

Con respecto a las implicaciones de la privacidad en esta rama del derecho anglosajón, Puente de la Mora señala que, a pesar de las características particulares y de la multiplicidad de fuentes del sistema legal estadounidense, resulta necesario recordar que todas las ramas del Derecho estadounidense operan en observancia a la Constitución Política, la cual *"se proclama a sí misma como la ley suprema de la nación"* (Puente de la Mora, 2007), por lo que dentro del ámbito constitucional, la única fuente aplicable viene a ser la constitución misma y sus enmiendas.

Asimismo, la autora apunta que a pesar de no encontrarse contemplado dentro del texto constitucional, el derecho a la privacidad ha sido considerado parte del sistema constitucional por la Corte Suprema a raíz de la interpretación de la Primera Enmienda Constitucional (que puede ser interpretada para salvaguardar el anonimato), la Tercera Enmienda Constitucional (que ha sido interpretada para proteger la privacidad del hogar) y la Cuarta Enmienda Constitucional (que protege el derecho de los individuos sobre su persona, casa y pertenencias *"sobre registros excesivos y embargos"* y que según Brandeis se dirige a la protección del *"derecho a ser dejado solo"* del individuo y no de los lugares en que se encuentren) *(Puente de la Mora, 2007, pág. 9).*

*Derecho Codificado*

A raíz de la toma de consciencia sobre la importancia de la privacidad existente durante los años sesentas y setentas, el Derecho codificado anglosajón fue adaptándose para proteger de mejor manera al individuo ante los excesos posibles con la llegada de nuevas tecnologías.

El primero de estos esfuerzos de adaptación puede ser encontrado en el reporte del Departamento de Salud, Educación y Asistencia Social en Estados Unidos que propone *"una especie de código que constituyera las Mejores Prácticas de Información, el cual consistía en una serie de principios básicos para preservar la privacidad de la información, que asignaba derechos y responsabilidades en la recolección y uso de la información personal" (Puente de la Mora, 2007, pág. 11)* y que contribuyeron a estructurar el derecho a la privacidad en los Estados Unidos.

Finalmente, se debe resaltar que a partir de la década de los años setenta, el Congreso de los Estados Unidos ha aprobado numerosas leyes relacionadas con la privacidad de los ciudadanos y que han tratado el tema tanto desde una perspectiva garantista como desde una perspectiva dirigida al fomento de la seguridad nacional, lo cual se estudiará con más detalle en capítulos posteriores de la presente investigación.

### *Derecho a la Información y Derecho de Autodeterminación Informativa*

Considerados ambos como derechos humanos en el mundo moderno[22], tanto el derecho a la información como el derecho de autodeterminación informativa se relacionan con el papel del individuo frente al uso y manejo de que de la información pueden realizar entes públicos y privados.

Ante esta situación, a continuación se dedicarán algunas páginas al estudio de ambos derechos; primeramente se tratará el derecho a la información, el cual inicialmente se fue caracterizado con base en los tres tipos de información reconocidos por este derecho (información privada, pública y de interés general), sus principios (tanto los ideales como los vigentes en el Derecho Público costarricense), sus elementos y la problemática que lo caracteriza.

En segundo lugar, se realizará un estudio similar sobre el derecho de autodeterminación informativa, para el cual se encontrará una definición, se estudiarán sus fundamentos, naturaleza jurídica y demás características, y finalmente se examinarán algunos de sus principios y elementos más característicos.

## El Derecho a la Información

[22] Debe aclararse en este punto que si bien la condición del derecho a la información como derecho humano resulta innegable en la actualidad, la caracterización del Derecho de Autodeterminación informativa como un derecho humano escindido por completo del Derecho a la Intimidad aún no ha sido reconocida por las Naciones Unidas. A pesar de esta situación, una gran cantidad de pronunciamientos y actos realizados por este ente internacional apuntan que nos encontramos frente a un proceso de reconocimiento progresivo que, tal como se verá más adelante, sigue el reconocimiento realizado por otros entes internacionales.
A lo largo de la presente investigación se mantendrá el postulado de que el derecho de autodeterminación informativa constituye efectivamente un derecho humano; quizá adelantándose al tiempo actual, según el juicio del suscrito investigador, pero previendo de la misma manera las tendencias que marcarán el futuro con base en las mareas de eventos que han caracterizado los últimos años.

El derecho a la información cobra relevancia para la presente investigación en tanto este derecho se relaciona de maneras particulares con el derecho a la intimidad, con el cual debe coexistir a pesar de encontrarse usualmente ambos derechos, en directa contraposición.

La relación entre ambos derechos, si bien es usualmente polarizada por las diversas tesis doctrinarias, no excluye la posibilidad de encontrar puntos intermedios entre información e intimidad. Estos puntos intermedios representan posibles soluciones a los problemas que se presentan al estudiar este derecho desde diferentes puntos de vista.

Desde el punto de vista democrático, el derecho a la información permite al individuo asegurar su libertad y dignidad, a la vez que le permite exigir la transparencia gubernamental, por medio de la superación del secretismo característico de los regímenes políticos opresivos. El derecho a la información representa para el individuo la posibilidad de saber, de ser titular de información y de poder utilizar tal información de las más diversas maneras, empoderándolo en democracia al tornarse consciente de aquellas informaciones que le afectan.

Al respecto, deben recordarse las palabras de James Madison, uno de los padres de la revolución estadounidense, quien plasmó la importancia de este derecho al afirmar que: *"Un gobierno popular sin información popular o con medios para que ésta sea accesible, constituye el prólogo de una farsa o de una tragedia, o quizás ambas cosas. El saber siempre debe gobernar la ignorancia; y la población que busca ser su propio gobernante debe proveerse a sí misma con el poder que el conocimiento trae consigo"* (Valladares Lanza, 2008, pág. 15).

El derecho a la información forma parte de los fundamentos que legitiman el uso individual de las nuevas tecnologías de la información y la comunicación. A pesar de lo

anterior, no debe olvidarse que desde el punto de vista de la intimidad y la privacidad, la información se presenta también como una potencial amenaza a la dignidad humana. Desde este punto de vista, el derecho a la información puede dar lugar a abusos tanto por parte de entes públicos como privados, abriendo las puertas a problemas tales como el mal uso de información confidencial y la exposición pública de los ámbitos privados del individuo, lo cual a su vez amenaza la dignidad humana al exponer al ser humano al escrutinio y rechazo público.

Ante este conjunto de elementos sin duda relevantes para tema en estudio, a continuación se realizará un breve estudio de aquellos conceptos que lo fundamentan, continuando con la definición del término, la caracterización de su naturaleza jurídica y de los principios que rigen este derecho, para concluir con la enumeración de algunos de sus elementos fundamentales.

### *Fundamentos y Definición del Derecho a la Información*

El derecho a la información, al igual que los derechos anteriormente estudiados, encuentra sus fundamentos en la dignidad humana y *"tiene sus raíces en la postura humanista de situar al hombre en la cúspide de todo ordenamiento jurídico, para que se le reconozcan una serie de derechos que se consideran fundamentales, sin cuyo reconocimiento y protección no podría desarrollarse el hombre como tal* (Valladares Lanza, 2008, pág. 9).

Este derecho, surgido a partir de las ideas de la Ilustración y las revoluciones liberales, es inicialmente considerado una manifestación de *"un espacio ciudadano protegido por el laissez faire impuesto al nuevo Estado Liberal"* (Veljanovich, 1997, pág. 4), el cual se ve

traducido con posterioridad en las diversas declaraciones de derechos individuales, las cuales cesan en su percepción de este como una libertad irrestricta del individuo y lo comprenden dentro de un ámbito de coexistencia social, a partir del cual la libertad pueda ser limitada.

Efectivamente, el derecho a la información, inicialmente concebido únicamente desde sus manifestaciones dentro del derecho a la libertad de prensa y libertad de expresión, gradualmente evoluciona en el marco de la *segunda revolución industrial,* el capitalismo de finales del siglo XIX y las guerras mundiales producidas en las primeras décadas del siglo XX, para ser finalmente reconocido y protegido por la Declaración Universal de Derechos Humanos en 1948, en su artículo 19, el cual reza:

*"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el difundirlas sin limitación de fronteras, por cualquier medio de expresión"* (Organización de las Naciones Unidas, 1948).

Tal como puede observarse en el articulado de la Declaración, el Derecho a la Información es concebido como parte de un conjunto complejo de derechos dentro de los cuales se encuentran: el derecho a no ser molestado a causa de sus opiniones; el derecho a investigar informaciones y opiniones; el derecho a recibir informaciones y opiniones, el derecho a difundir informaciones y opiniones, entre otros (Veljanovich, 1997, pág. 8).

Este conjunto de derechos posee, a pesar de su amplitud, límites, que en palabras de Córdoba Ortega se encuentran en *"todas aquellas situaciones relacionadas íntimamente con la vida privada de las personas, incluyendo dentro de éstos derechos el honor, la imagen y*

*el prestigio, así como el secreto de Estado y aquellos documentos que son declarados confidenciales por ley"* (Córdoba Ortega, 1996, pág. 33).

Ahora bien, la comprensión de la acepción del derecho a la información se encuentra fundamentalmente marcada por la definición del concepto *"Información"* al ser este el objeto que busca garantizar dicho derecho al individuo. Una primera definición genérica del concepto es presentado por Valladares Lanza, quien define este concepto como *"la comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una determinada materia y emplea los procedimientos para acopiar, almacenar, tratar, difundir, recibir; así como los tipos, hechos, noticias, datos, opiniones, ideas y sus diversas funciones"* (Valladares Lanza, 2008).

Este concepto genérico de información debe ser a su vez definido, al comprenderse, dadas las limitaciones actualmente establecidas a este derecho, que no resulta posible para el individuo en sociedad pretender el acceso a toda la información disponible, especialmente debido a los roces que tal conducta generaría con el derecho a la intimidad de sus conciudadanos.

Así, resultará posible seguir el ejemplo de Beatriz Boza, quien comprende la posibilidad de subdividir la información en tres clasificaciones fundamentales, a saber: información privada, información pública e información de interés general.

*Información Privada*

De conformidad con lo estudiado con anterioridad, la información privada es aquella concerniente a la vida, que se encuentra protegida por sus derechos a la intimidad y a la privacidad; se puede identificar de manera amplia con aquella información relacionada con la *"vida privada"* o *"esfera privada"* individual, las creaciones intelectuales del sujeto o aquella que pueda encontrarse en bases de datos privadas o públicas que contenga datos personales de un individuo (Boza, 2004, pág. 2).

Parafraseando a Réniz Caballero, citada por Boza, si bien es aceptado que el objeto del derecho a la información es *"la información veraz e imparcial"* (Boza, 2004, pág. 2), no debe olvidarse que dicha información tiene un poseedor, independientemente de si se encuentra en manos de un ente público o privado, por lo que no puede un tercero disponer de ella sin autorización de su titular.

Según Boza, el reconocimiento del estatus patrimonial de esta información tiene como consecuencia que esta se torna susceptible de una valoración económica y, pese a ser un derecho exclusivo, absoluto, perpetuo, ilimitado e inviolable del individuo, es un bien *"susceptible de actos de uso, disfrute, disposición y reivindicación"* (Boza, 2004, pág. 3) que no puede ser divulgado abiertamente por un tercero, alegando para ello su derecho a la información.

### *Información Pública*

Velasco Caballero, citado por Boza, define este concepto al establecer que *"es pública la información que procede del Estado… y es Privada la información que proviene de los particulares y sus asociaciones" (Boza, 2004, pág. 4).* La Información Pública no es

considerada por la doctrina como propiedad del Estado, al entenderse usualmente que esta pertenece a todos los ciudadanos de una nación, quienes, constituidos en una especie de copropiedad, pueden hacer efectivo el uso y disfrute de esta al exigir al Estado y sus entidades el acceso a tal información.

Este derecho de acceso a la información pública solamente puede ser limitado por aquellas disposiciones dirigidas a la protección de la información privada que se encuentre en manos del Estado. Asimismo, tal como se estudiara con anterioridad, la ley de una nación puede disponer restricciones sobre el acceso a ciertas informaciones públicas, en los calificados casos en que se considere que tal información pudiera vulnerar la seguridad nacional.

*Información de Interés General*

Es definida por Boza como *"aquella información que, si bien no beneficia a la totalidad de una comunidad, es relevante a "una fracción muy importante de los miembros de ésta"" (Boza, 2004, pág. 5)* y que hace referencia a aquella información que, pese a su carácter privado, resulta relevante a los intereses de la comunidad, por lo que es trasladada de la esfera privada a la pública, no sin antes haber analizado específicamente las características del titular de la información privada y de la naturaleza de dicha información, con miras a garantizar que el traslado sea realizado de manera legítima.

*Definiciones de Derecho a la Información*

El derecho a la información posee múltiples acepciones que hacen referencia a sus diferentes vertientes. En este contexto, la formulación de una definición inequívoca para el derecho a la información resulta sumamente difícil. A pesar de ello, con miras a brindar una primera definición que ubique al lector sobre el significado de este derecho, puede afirmarse que el derecho a la información hace referencia al derecho genérico del individuo a "saber" y que para los intereses de la presente investigación, deberá ser entendido en contraposición con el derecho individual a la intimidad (que implica la posibilidad de excluir a otros de "saber" sobre nosotros).

Este derecho del individuo puede, por supuesto, ser definido con mayor especificidad. Así, por ejemplo Boza lo define *"como el derecho a participar en los procesos de comunicación, y por lo tanto el derecho de recibir, transmitir y difundir información"* (Boza, 2004, pág. 1), mientras que Jorge Carpizo y Ernesto Villanueva, citados por Valladares Lanza, consideran que de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos, *"es la garantía fundamental que toda persona posee a traerse información, a informar y a ser informada " (Valladares Lanza, 2008, pág. 7).*

Por su parte, Veljanovich establece que *"este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el difundirlas sin limitación de fronteras, por cualquier medio de expresión"* (Veljanovich, 1997, pág. 8) a la vez que Días Cafferata considera que *"es la facultad que tiene todo ciudadano, como consecuencia del sistema republicano de gobierno, de acceder a todo tipo de informaciones en poder tanto de entidades públicas como de personas privadas que ejerzan funciones públicas o*

*reciban fondos del Estado, con la consecuente obligación estatal de instrumentar un sistema administrativo que facilite a cualquiera la identificación y el acceso a la información solicitada"* (Días Cafferata, 2009, pág. 154).

Por último, y de conformidad con la definición anterior, es valiosa la definición realizada por Córdoba Ortega, quien recuerda al lector que dentro de la doctrina constitucional, el derecho a la información ha sido considerado también como *"una modalidad del derecho de peticionar a las autoridades: aquella por la cual se requiere del Estado de la publicidad de los actos públicos (está implícito en la forma republicana de gobierno) y de la información que alcance el interés público"* (Córdoba Ortega, 1996, pág. 29).

### *Naturaleza Jurídica y Principios del Derecho a la Información*

Según Aguilar Bulgarelli, el derecho a la información *"Se enmarca dentro de los derechos subjetivos omisivos, pues se constituye en un comportamiento agraviante para la libertad de los individuos (conocidas como garantías individuales. La consecuencia de que el Estado no cumpla con dichas libertades, trae consigo la responsabilidad del mismo por el agravio cometido"* (Aguilar Bulgarelli, 1996, pág. 39).

Este derecho, al igual que otros derechos fundamentales, posee como sujeto a todo ser humano, a pesar de lo cual el objeto de dicho derecho (la información) *"no es universal, sino general, por que admite excepciones en la difundibilidad" (Villalobos Quirós, 1997, págs. 54-55).* Ante esta situación, no constituirá violación al derecho su limitación por razones tales como que la información esté fuera de circulación (que no se

encuentre a disposición del ente requerido a liberarla), que la obtención, manejo o publicación de la información en cuestión afecte otro derecho fundamental, o que la información que se intente publicar bajo la protección de este derecho no cumpla con los requisitos de veracidad necesarios.

Asimismo, al igual que en el caso del derecho a la intimidad, el derecho a la información puede ser comprendido en una doble perspectiva, que lo comprende tanto en su función de derecho subjetivo, a disposición del sujeto para su reclamación, como en su función de bien jurídico tutelado; la información se constituye en un elemento fundamental para el adecuado funcionamiento de todo Estado Social de Derecho, al garantizar al ciudadano el ejercicio del control social y político sobre la actividad estatal.

En esta doble perspectiva, debe entenderse que en la actualidad se llegan a mezclar las funciones del individuo y el Estado con respecto a la tutela del derecho a la información; el Estado se ve obligado a establecer los mecanismos y garantías procesales necesarios, para asegurar al ciudadano la correcta tutela de la completa gama de derechos involucrados con el derecho a la intimidad y asegurando a su vez el ejercicio negativo de este, estableciendo y asegurando la puesta en práctica de los límites legales a este derecho; en especial en aquellos casos en los cuales su ejercicio afecte negativamente los derechos fundamentales de otros ciudadanos.

*Principios del Derecho a la Información*

Tal como se ha estudiado, el derecho a la información posee diversas vertientes que se relacionan con la posibilidad del individuo de recabar, manejar y divulgar información en sus relaciones con entes públicos o privados. Dada esta circunstancia, a continuación se realizará primeramente una breve enumeración de aquellos principios que, según la UNESCO, deberían fundamentar la legislación de todo país con un régimen legal dirigido al respeto al derecho a la información; para a continuación exponer aquellos principios relacionados con el derecho al acceso a la información vigentes en la actualidad en el contexto jurídico del Derecho Público costarricense.

## Principios Ideales del Derecho a la Información

Según Mendel, dado que el derecho a la información es un derecho fundamental garantizado por el derecho internacional, resulta posible establecer ciertos principios que, al ser adoptados por los Estados, garanticen el reconocimiento de este. Para ello, el autor recomienda la adopción de los nueve principios establecidos por la Organización no Gubernamental (ONG) Artículo 19, en materia de Libertad de Información (Mendel, 2009); a saber:

- Transparencia Máxima*:* Derivado de las características mismas del derecho a la información, *"implica que el alcance del derecho a la información debe ser tan amplio como la gama de información y entidades respectivas, así como los individuos que puedan reclamar el derecho, buscándose que idealmente toda la información pública o de interés público sea accesible por todo individuo interesado" (Mendel, 2009, pág. 39)*.

- Obligación de Publicar: El cual establece que las entidades públicas no deben limitarse a la mera aceptación de solicitudes de información por parte del público, sino que deben adoptar un enfoque activo en el tema, publicando y difundiendo activamente información clave aún en ausencia de solicitudes (Mendel, 2009, pág. 41).
- Promoción del Gobierno Abierto: Principio que busca la eliminación del secreto gubernamental con base en la promoción de un cambio cultural, la educación del público y el establecimiento de penalidades a la obstrucción del acceso a la información (Mendel, 2009, pág. 42).
- Limitación a las Excepciones: Busca el establecimiento de definiciones claras y exigentes de las limitaciones al derecho a la información, procurando la eliminación de límites genéricos y difíciles de determinar (tal como la invocación genérica de la "seguridad nacional" sin determinar exactamente el tipo de daño que podría causarse) pero contemplando apropiadas salvaguardas a los derechos fundamentales cuya vulnerabilidad sea debidamente comprobada (Mendel, 2009, pág. 43).
- Facilitación del acceso: El cual procura el establecimiento de estándares de oportunidad y justicia para la tramitación de toda solicitud de información que logre la simplificación de los procesos, buscando que estos lleguen a ser sencillos, rápidos y gratuitos o de bajo costo (Mendel, 2009, pág. 46).
- Disminución de costos: Que requiere la eliminación de barreras monetarias de acceso a los procesos de solicitud de información (Mendel, 2009, pág. 48).

- Reuniones abiertas: Que requiere a las entidades públicas la publicación de la información de sus sesiones al público para su examen y control (Mendel, 2009, pág. 48).
- La precedencia de la transparencia: El cual exige de los Estados la modificación o eliminación de aquellas leyes inconsistentes con el principio de transparencia máxima, con miras a garantizar el derecho a la información a mediano y largo plazos (Mendel, 2009, pág. 49).
- Protección para denunciantes[23]: En el cual se solicita a los Estados que garanticen a los diversos funcionarios públicos que no se encontrarán sujetos a sanciones, por liberar, de buena fe, información relacionada con actos incorrectos o que amenacen la salud, seguridad o ambiente, realizados por la administración pública; salvo cuando tales sanciones cumplan intereses legítimos y sean necesarios en una sociedad democrática, con lo cual se fomenta el flujo de información al público y la transparencia (Mendel, 2009, pág. 50).

## Principios Relacionados con el Derecho al Acceso a la Información, Vigentes en el Marco del Derecho Público Costarricense

[23] De suma relevancia en el contexto actual de las telecomunicaciones convergentes, en el cual se ha visto surgir a la luz pública escándalo tras escándalo relacionado con violaciones por parte de los estados a los derechos fundamentales de los ciudadanos del mundo (ver revelaciones de Wikileaks, Snowden, entre otros) que no solamente no han sido reconocidos oficialmente por los Estados, sino que han culminado con el encarcelamiento o extrañamiento de hecho de los denunciantes.

Con respecto a los principios fundamentales de este derecho en el ámbito del Derecho Público costarricense, debe citarse a Córdoba Ortega, quien ha realizado una excelente clasificación de los ellos dentro del marco jurídico costarricense. Según el autor, los principios que para el ejercicio de este derecho ante la administración pública costarricense deben cumplirse, son los principios de legalidad, de transparencia administrativa, de igualdad, de publicidad, democrático, de eficiencia, de razonabilidad y proporcionalidad y de especialidad.

- Principio de Legalidad: Establece los límites y alcances de la Administración en conformidad con el ordenamiento jurídico. Según Córdoba Ortega, este principio se encuentra desarrollado en el artículo 11 de la Constitución Política de Costa Rica y los artículos 11.1 y 13.1 de la Ley General de la Administración Pública, en los cuales se entiende *"como un sometimiento expreso de la Administración Pública al ordenamiento jurídico, implicando necesariamente que los órganos públicos solo podrán hacer aquello que la norma le permita" (Córdoba Ortega, 2004, pág. 8)*.
- Principio de Transparencia Administrativa: El cual responde a la concepción del Estado Social de Derecho al someter la totalidad de las actuaciones de la Administración Pública al control ciudadano, exponiéndolas a responsabilidad en caso de cometer infracciones. Este principio se encuentra plasmado en el segundo párrafo del artículo 11 de nuestra Constitución Política, así como en los artículos 27 y 30 de esta (Córdoba Ortega, 2004, pág. 11).
- Principio de Igualdad: Protegido por el artículo 33 de nuestra Carta Magna, procura brindar a toda persona *"igualdad al accesar y peticionar información de*

*naturaleza pública ante las autoridades públicas"* (Córdoba Ortega, 2004, pág. 16), en un marco que exige de la ley la consideración equitativa de los intereses de todo individuo, junto con la no discriminación y el respeto a la dignidad humana, examinando la aplicación de este principio en cada caso concreto.

- Principio de Publicidad: El cual pretende asegurar a todo ciudadano su capacidad de conocer *"tanto el ordenamiento jurídico que lo rige, como el sustento de las actuaciones de la Administración" (Córdoba Ortega, 2004, pág. 18).* Puede encontrarse el fundamento constitucional de este derecho, según el autor, en los artículos 124, 126 y 129 de la Constitución Política de Costa Rica (y con respecto a la publicación de las leyes el Reglamento de la Asamblea Legislativa).
- Principio Democrático: Consagrado según Córdoba Ortega en los artículos 1 y 9 de nuestra Constitución Política, en los cuales se establecen los fundamentos del sistema de gobierno de nuestro país, se caracterizado por ser democrático, libre, independiente, popular, representativo, participativo, alternativo y responsable, ejercido por el pueblo y tres Poderes distintos e independientes entre sí (Córdoba Ortega, 2004, pág. 21).

### *Elementos del Derecho a la Información*

Según Martí de Gidi, el derecho a la información posee tres dimensiones básicas que se pueden entender en referencia a tres ámbitos de aplicación de este derecho: el ámbito individual, el ámbito colectivo o abstracto, y el ámbito general.

La primera de las dimensiones señaladas por la autora, hace referencia al conjunto de derechos individuales que conforman el derecho a la información y que se identifican con el derecho individual a ser titular activo del derecho a la información (el derecho a saber sobre un hecho de manera directa y a ser titular de este).

La segunda dimensión hace referencia a la debida *"garantía institucional de la opinión pública libre"* (Martí de Gidi, 2001, pág. 8), la cual debe ser entendida como la apreciación o el parecer que sobre una determinada cuestión existe en la colectividad, y que determina el pluralismo político en una sociedad democrática. Parafraseando a Francesc de Carreras, citado por Martí de Gidi, la opinión pública debe ser entendida como aquella formada en la base de la sociedad y no en la élite gobernante y que debe tener *"al menos, la posibilidad y la perspectiva de ser eficaz, de tener una influencia real en los centros de poder de decisión política de un país. Si no hay esta posibilidad, no existe opinión pública, ya que esta falta de eficacia impide que se forme y se desarrolle"* (Martí de Gidi, 2001, pág. 8).

La tercera y última dimensión mencionada por la autora, hace referencia a la garantía institucional que debe brindar el Estado en referencia al libre ejercicio de los medios de comunicación en sus labores de información a la sociedad en general, para lo cual el Estado deberá "dotarlos de derechos instrumentales".

Dentro de las tres dimensiones señaladas, es relevante para la presente investigación la aclaración de aquellos derechos que se constituyen en elementos del derecho individual a la información, los cuales han sido recopilados elocuentemente por Nogueira Alcalá (citado por Martí de Gidi), a partir del estudio de la Convención Americana de Derechos Humanos y los textos constitucionales de América Latina.

Según el autor, el derecho a la información comprende, para quien informa, los siguientes derechos (Martí de Gidi, 2001, pág. 9):

a) *Derecho a investigar y buscar informaciones y opiniones;*

b) *Derecho a difundir informaciones de relevancia pública por cualquier medio y opiniones.*

c) *Derecho a emitir informaciones u opiniones;*

d) *Derecho a no ser censurado ni objeto de restricciones preventivas en forma explícita o implícita, directa o indirecta, a excepción de medidas destinadas a proteger la moral de los menores o adolescentes o en casos de estados de excepción constitucional;*

e) *Derecho de acceso a las fuentes de información;*

f) *Derecho al secreto profesional periodístico y a la reserva de las fuentes.*

g) *Derecho a la cláusula de conciencia;*

h) *Derecho al acceso y utilización de los instrumentos y medios naturales o tecnológicos necesarios que permitan emitir las opiniones o informaciones.*

Y con respecto al informado, señala el Doctor Nogueira Alcalá los derechos siguientes:

a) *Derecho a recibir opiniones e informaciones.*

b) *Derecho a seleccionar la información que recibe y los medios a través de la cual recibirla.*

c) *Derecho a ser informado veraz y oportunamente.*

d) *Derecho a que sea preservada su honra y vida privada.*

e) *Derecho a rectificación o respuesta;*

f) *Derecho a solicitar la imposición judicial de responsabilidades civiles y penales en los casos determinados por el ordenamiento jurídico.*

### *Problemática del Derecho a la Información*

A pesar de tener el potencial de asegurar al individuo una multiplicidad de derechos relacionados con aspectos positivos de su vida democrática, el derecho a la información presenta un problema fundamental, relacionado con el acceso, transmisión y manipulación de información, tanto pública como privada, que es posibilitada por este derecho, el cual implica una serie de vulnerabilidades y peligros de diversas índoles para el individuo.

En palabras de Garriga Domínguez: *"Tanto en el ámbito de las Administraciones Públicas, como en el de las entidades privadas, en las sociedades desarrolladas se recaban, almacenan y tratan un gran número de informaciones sobre millones de personas relativas a multitud de facetas de su vida. Estos datos son recogidos con las más diversas finalidades: gestión de clientes, gestión de cobros y pagos, selección de personal, historiales clínicos, tarjetas de crédito, educación, seguros de vida y salud, investigación, etc. En demasiadas ocasiones, basándose exclusivamente en esos datos registrados en ficheros informáticos se adoptarán decisiones que afectarán directa o indirectamente a las personas a las que éstos se refieren.*

*El actual desarrollo de las tecnologías de la información, hace posible recoger y almacenar, sin límite de espacio, infinidad de datos sobre un mismo individuo, realizar un auténtico catálogo de informaciones personales sobre él y además interrelacionar todos los datos existentes sobre*

*una misma persona, con independencia de que se encuentren en archivos distintos, relativos a diferentes etapas de su vida, o que estos hayan sido recogidos incluso en lugares lejanos. Se puede acumular sin límite la información y recabarla en cuestión de segundos con independencia de la distancia a la que se encuentre. Pero, ¿para qué se va a utilizar esa información?"* (Garriga Domínguez, 2009, pág. 26).

Tal como correctamente lo señalan Garriga Domínguez y Víctor Bazán, el principal problema que genera el derecho a la información no se presenta en el mero ejercicio del derecho a la información o en el uso de las nuevas tecnologías de la información y la comunicación; *"la dificultad aparece cuando dicho uso informático se convierte en abuso informático" (Bazán, 1999, pág. 17)* y cuando el derecho a la información facilita a entes públicos y privados por igual el abuso de su facultad de recolección y tratamiento de la información.

Finalmente, debe recordarse que el abuso del derecho a la información posee la capacidad de afectar seriamente tanto la integridad y dignidad individual como los fundamentos mismos de nuestro sistema democrático. Tal como se estudiará más adelante, la información de todo individuo es, por su naturaleza misma, contextual y relacional; por lo que aún elementos informacionales aislados y aparentemente insignificantes, al ser reunidos poseen la capacidad de generar un verdadero perfil de la persona, el cual, en caso de ser expuesto a la mirada pública, *"podría degenerar en el más implacable fenómeno de control y manipulación social que pueda imaginarse" (Pérez Luño A. , 1992)*.

## El Derecho de Autodeterminación Informativa

Perfilado como un nuevo derecho que busca solucionar el dilema existente entre el necesario manejo de información y el derecho a la intimidad, el derecho de autodeterminación informativa busca brindar al individuo un ámbito amplio de control sobre aquella información que haga referencia a su persona, sin limitarse únicamente a los aspectos más próximos, secretos o sensibles de su vida, como tradicionalmente sucede en el derecho a la intimidad.

Al poseer mayor flexibilidad y ámbito de aplicación, este derecho admite que *"el tratamiento de la información personal puede, pero no tiene porque, afectar a informaciones íntimas o secretas que son el objeto de protección del derecho a la intimidad"* y que *"los datos personales informatizados no tienen necesariamente que precipitar un retrato personal que implique una valoración peyorativa u ofensiva de un individuo y que atente contra su buen nombre o fama" (Garriga Domínguez, 2009, pág. 24)* por lo que facilita al individuo la protección positiva que no le brinda la visión tradicional del derecho a la intimidad y reconoce, en palabras del Tribunal Constitucional Alemán, *"la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida"* (Garriga Domínguez, 2009, pág. 32).

Así, siguiendo a Chirino Sánchez, puede afirmarse que la autodeterminación informativa no trata *"de limitar el tratamiento electrónico de los datos que es, en esencia, (…) una condición para el progreso de los Estados, sino más bien de luchar por que dicho tratamiento se realice de una manera democrática, afianzando los derechos y garantías del*

*ciudadano, y promocionando la participación social de todos los seres humanos"* (Chirino, 1997, pág. 17), por lo que puede concluirse esta introducción al tema recordando, - tal como lo hizo Chirino - a Gerard Dronsch, quien afirmó que, en la sociedad de la información, *"El ser humano "no automático" debe ser protegido en un mundo que se automatiza" (Chirino, 1997, pág. 19).*

### *Definición y Fundamentos del Derecho de Autodeterminación Informativa*

En respuesta a las limitaciones de la visión tradicional del derecho a la intimidad ante el desarrollo de las tecnologías de la información y la comunicación, el derecho de autodeterminación informativa se presenta como *"una nueva vestimenta para un viejo derecho humano: el derecho a la privacidad, a controlar al poderoso Estado, a controlar que éste no afecte a quienes se encuentran bajo su poder y a quienes se encuentran sometidos a sus amenazantes intervenciones"* (Hassemer & Chirino, 1997, pág. 167).

Los antecedentes del derecho de autodeterminación informativa pueden ser encontrados, según Peña Ortiz y Achío Gutiérrez, en la doctrina germana, la cual *"proclama el desarrollo de la personalidad desglosándolo en dos libertades básicas: una libertad general de acción que permita decidir la realización u omisión de determinados actos y la facultad para comportarse o actuar de acuerdo con esa decisión; y la autodeterminación informativa que se refiere a la libertad para determinar quién, qué y con qué ocasión pueden conocer informaciones que conciernen a cada* sujeto" (Peña Ortiz & Achío Gutiérrez, 2011, pág. 26).

En palabras de Chirino, este derecho surge a partir del choque de las necesidades de acceso a la información y transparencia de las instituciones públicas contra *"la necesidad de tutelar a la persona frente al uso desmedido de sus datos personales" surgidas en la actual sociedad de la información y el conocimiento"* (Chirino, 1997).

En este contexto, el derecho de autodeterminación informativa encuentra sus primeras afirmaciones en la ya mencionada sentencia del Tribunal Constitucional Alemán sobre la Ley del Censo de Población de 15 de diciembre de 1983[24]; entiende *"al derecho a la intimidad como expresión del derecho a la autodeterminación informativa"* (Bazán, 1999) y critica duramente la laxa protección brindada anteriormente a la intimidad individual por la "*teoría de las esferas de la personalidad"* al reconocer que la *"interacción libre y democrática de los individuos en una sociedad cada vez más compleja, no parte de una tutela de esferas de intimidad, sino más bien del reconocimiento de la necesidad de que el sujeto decida sobre quién, cuándo, dónde, y bajo qué circunstancias puede tomar contacto con sus datos personales"* (Hassemer & Chirino, 1997, pág. 131).

Mediante estos nuevos presupuestos, da inicio un proceso internacional de creación legislativa (ejemplificado por la Ley de protección de datos del Land Hesse de 1970; la Datalag sueca de 1973; la Constitución portuguesa de 1976; la Constitución Política española de 1978; la Ley de Informática, Ficheros y Libertades francesa de 1978; la Ley austriaca 565 de 1978; la Ley Italiana 121 de 1981; la Data Protection Act inglesa de

[24] Según Rojas Mora, la citada sentencia del Tribunal Constitucional Alemán puede resumirse recordando que buscaba realizar un análisis de constitucionalidad de la Ley de Censos, la cual pretendía la realización de un censo nacional obligatorio en el que "se entrevistara a todos los ciudadanos alemanes sobre información tal como su nombre, edad, trabajo, inclinaciones políticas, religiosas, familiares, ingresos, gustos, dirección y otra enorme cantidad de datos de índole meramente personal, so pena de sufrir fuertes sanciones económicas. Según los autores, la sentencia ataca la recolección de datos individuales desde dos flancos fundamentales: el peligro del control cruzado de datos y la obligación de la entrega de la información" (Rojas Mora, 2007, pág. 43).

1984; y la Ley Alemana Federal de Protección de Datos de 1990), que culmina con la emisión de la Carta de los Derechos Fundamentales de la Unión Europea, la cual consagra el derecho de autodeterminación informativa como derecho fundamental.

En nuestro país, el derecho de autodeterminación informativa no se encuentra contemplado expresamente por nuestro marco constitucional[25] actual, a pesar de lo cual, la jurisprudencia de nuestra Sala Constitucional ha sido enfática en la afirmación de su existencia (basándose para ello en la existencia de fundamentos a este en los artículos 1, 24, 30, 33, 41 y 77 constitucionales) al definirlo en su sentencia número 4847-99 de las 16 horas 27 minutos del 22 de junio de 1999 como:

*"(…) el derecho fundamental de toda persona física o jurídica a conocer lo que conste sobre ella, sus bienes o derechos en cualquier registro o archivo, de toda naturaleza, incluso mecánica, electrónica o informatizada, sea pública o privada; así como la finalidad a que eta información se destine y a que sea empleada únicamente para dicho fin, el cual dependerá de la naturaleza del registro en cuestión. Da derecho también a que la información sea rectificada, actualizada, complementada o suprimida, cuando la misma sea incorrecta o inexacta, o esté siendo empleada para fin distinto del que legítimamente puede cumplir. Es la llamada protección a la autodeterminación informativa de las personas, la cual rebasa su simple ámbito de intimidad"* (Peña Ortiz & Achío Gutiérrez, 2011, pág. 28).

De esta manera, se puede observar cómo insiste nuestra Sala Constitucional en reforzar la diferenciación de este derecho respecto a la concepción tradicional del derecho a la intimidad, al establecer, en su voto 4847-99 el deber del Estado de extender su actuar a partir de la intimidad y *"controlar y regular el uso de los datos de las*

[25] Mas sí se encuentra presente en los contenidos de la Ley Nº8968 (Asamblea Legislativa de la República de Costa Rica, 2011) y su reglamento (Poder Ejecutivo de la República de Costa Rica, 2013).

*personas (sean íntimos o no)"* (Peña Ortiz & Achío Gutiérrez, 2011, pág. 23)*;* a la vez que manifiesta en su sentencia 5892-99 del 27 de julio de 1999 que:

*"(…) en la medida en que los ciudadanos puedan alcanzar un control sobre las informaciones que sobre sí mismos circulan en todos los ámbitos, en la misma medida podrá alcanzar las condiciones para evitar que el Estado o los particulares lo conviertan en una mera pieza del engranaje del poder, rebajándolo, en tal supuesto, a gozar de los ámbitos de libertad que el Estado quiera otorgarle y no aquellos que le corresponden como persona titular de una dignidad irreductible. Esto ha producido que la doctrina constitucional se haya ocupado de un viejo derecho con un nuevo ropaje en la era tecnológica: se trata nada menos que del derecho a la privacidad y a la dignidad en el ropaje de la hoy muy discutida y analizada autodeterminación informativa"* (Peña Ortiz & Achío Gutiérrez, 2011, pág. 29).

Esta revisión de los fundamentos del derecho a la autodeterminación informativa permite ahora recordar la concreta definición que sobre este derecho presenta Víctor Bazán, quien establece que:

*"El derecho de autodeterminación informativa consiste en la posibilidad que tiene el titular de datos personales de controlar quiénes serán destinatarios de éstos y qué uso les darán, y se ejercita genéricamente a través de los derechos de acceso, rectificación y cancelación. Además, ofrece una textura que resulta acorde con los modernos desafíos informáticos, puesto que, abandonado el concepto de intimidad como libertad negativa, permite avanzar hacia una fase activa del proceso de circulación de la información personal, brindando protagonismo al interesado al posibilitarle el ejercicio de un adecuado control sobre la misma"* (Bazán, 2011, pág. 111).

Y finalmente, se puede concluir recordando la caracterización que, sobre la autodeterminación informativa presenta Herrán Ortiz, quien sugiere *"(…) una*

*conceptuación del derecho a la autodeterminación informativa que extienda su protección al uso ilícito o abusivo de la informática, frente a cualquier información en "manos de terceros" que represente una amenaza para la persona; la interceptación no consentida de la información, debe controlarse y limitarse sin detenerse a averiguar la índole íntima o no de la información. Así, pues, el fundamento último del derecho a la autodeterminación informativa consiste no en preservar ocultos y aislados del conocimiento ajeno los actos y vivencias de la realidad personal, sino en mantener la libertad y la dignidad del individuo, evitando la fiscalización interesada de la vida de las personas y, a través de ello, impedir la instrumentalización del ser humano"* (Herrán Ortiz, 2002, pág. 54).

### *Naturaleza Jurídica y Características del Derecho de Autodeterminación Informativa*

Tal como se estudiara con anterioridad, derecho de autodeterminación informativa presenta fundamentalmente *"un profundo arraigo en principios tales como la dignidad humana, la libertad individual, la autodeterminación y la democracia, que antes de ser utilizados como puntos de sustentación vacíos y sin contenido, adquieren una nueva perspectiva en el Estado de Derecho" (Chirino, 1997, pág. 18).*

El Derecho de autodeterminación informativa es, según Garriga Domínguez, un derecho instrumental o derivado *(Garriga Domínguez, 2009, pág. 19)*; tal posición debe ser reconocida tomando en consideración que nos encontramos ante un derecho que fundamentalmente busca dar "sentido y operatividad a la personalidad ante una visión "postinformática" de los derechos de Intimidad, Privacidad e Información" (Millán Salas & Peralta Ortega, 1995, pág. 215).

A pesar de su carácter derivado, debe afirmarse que el derecho de autodeterminación informativa puede ser considerado aún como un derecho fundamental en tanto, tal como afirma Lucas Murillo de la Cueva, *"nada impide la consideración como derecho fundamental de un derecho instrumental: en último caso todos lo son respecto de la dignidad humana"* (González Murúa, 1994, pág. 10); por ello, puede concluirse, junto con Bazán, que se está ante *"un derecho autónomo con doble dimensión: sustancial (derecho en sí mismo) e instrumental (soporte para cobertura de otros derechos)"* (Bazán, 2011, pág. 117).

Debe resaltarse que para el correcto estudio de la naturaleza jurídica del derecho de autodeterminación informativa es necesario comprender que, ante el peligro que representa la agresión informática, todos los derechos pueden verse afectados[26]. Por tal situación, más allá de buscar proteger la totalidad de los derechos expuestos, el derecho de autodeterminación informativa procura la protección de un único bien jurídico: la libertad individual (enfocada específicamente sobre su información personal[27]).

Para Riande Juárez, citado por Bazán, la protección de la información personal es llevada a cabo por este derecho mediante el establecimiento de responsabilidades tanto para el Estado como para el individuo. Según este autor, una correcta tutela de

[26] González Murúa, expone esta situación al reconocer que *"Un dato erróneo u obtenido de manera ilícita, por ejemplo, puede vulnerar el principio de igualdad, el derecho a la intimidad, el derecho de asociación o el derecho de educación, entre otros, pero también el derecho a obtener un empleo, el derecho a obtener una prestación de la Seguridad Social, o el derecho a la concesión de un préstamo por citar algunos"* (González Murúa, 1994, pág. 10).

[27] Efectivamente, este derecho procura asegurar la protección de la capacidad de decisión y el libre albedrío que posee el individuo sobre su información personal. En otras palabras, nos encontramos ante un derecho que procura eliminar el pesar causado al individuo por el peligro siempre presente de que sus datos personales sean tratados sin su consentimiento (o que como resultado de dicho tratamiento sus intereses se vean negativamente afectados).
Al proveer al individuo con una serie de garantías negativas y positivas capaces de reducir la amenaza de verse perjudicado por el tratamiento de sus datos personales, el individuo se encontrará libre de fenómenos como la censura (o la auto censura) relacionada con el comportamiento cauteloso de quien se sabe constantemente observado (por no decir en peligro).

este derecho implica que el establecimiento de los criterios de manejo de los datos y el ejercicio del control de este manejo, será dejado en las manos de la sociedad en general (y por tanto en los organismos estatales creados para tal fin), mientras que al individuo le es reconocido su derecho a brindar o no su consentimiento sobre el tratamiento de sus datos *(Bazán, 2011, pág. 111)*.

Asimismo, puede establecerse que la tutela de este derecho contiene dentro de su naturaleza misma tanto elementos negativos como positivos. Según Garriga Domínguez, los elementos negativos de la autodeterminación informativa no buscan prohibir el tratamiento de los datos personales, sino el establecimiento de cautelas y límites capaces de prevenir los riesgos del tratamiento de la información personal y que sean capaces de reparar los daños que esta actividad origine, intentando con ello *"conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información" (Garriga Domínguez, 2009, pág. 37)*.

Los principios positivos de la autodeterminación informativa conllevan por su parte el otorgamiento al individuo de un *"haz de facultades, poderes y potestades que (…) garantizan a las personas la posibilidad de ejercer un control efectivo sobre el uso y destino de sus datos" (Garriga Domínguez, 2009, pág. 39),* sin los cuales el elemento negativo quedaría vacío de contenido y su titular desamparado ante los abusos en el tratamiento de sus datos.

Según Garriga Domínguez, el elemento positivo de la autodeterminación informativa permite al individuo el *"imponer a terceros la realización u omisión de determinados comportamientos" (Garriga Domínguez, 2009, pág. 39)*, a la vez que conforma el

denominado *"habeas data" o "habeas scriptum",* el cual se estudiará con mayor detenimiento en el capítulo segundo.

Adicionalmente, debe señalarse que, el derecho de autodeterminación informativa podrá ser extendido a la totalidad del proceso de obtención y almacenamiento de los datos, tanto en su aspecto positivo como en su aspecto negativo, y no se encontrará limitado por la forma de almacenamiento de los datos (manual o electrónica) *(Bazán, 2011, pág. 112)*.

A pesar de su amplitud, debe recordarse que al hablar sobre derecho de autodeterminación informativa no se hace referencia a una garantía ilimitada del individuo que le brinde *"poder absoluto e ilimitado sobre sus datos" (Hassemer & Chirino, 1997, pág. 177)* ya que, *"su límite viene marcado por el valor de la información como bien colectivo en el conjunto social" (Bazán, 2011, pág. 120).*

A pesar de lo anterior, resulta posible reconocer que las limitaciones a este derecho tampoco pueden superar o negar la tutela de este derecho al individuo, por lo cual resulta posible identificar ciertos elementos que deberá cumplir cualquier limitación para ser considerada como legítima. Estos elementos son, según Hassemer & Chirino: el satisfacer un interés público preponderante, el tener un fundamento legal que cumpla con el principio de proporcionalidad y *"del principio emanado de la idea del Estado de Derecho que ordena la definición y puesta en vigencia de normas claras y precisas"* (Hassemer & Chirino, 1997, pág. 177).

*Elementos y Principios del Derecho de Autodeterminación Informativa*

Tal como se estableció anteriormente, el derecho de autodeterminación informativa posee un elemento positivo y un elemento negativo, los cuales fundamentan aspectos básicos de la praxis del derecho en cuestión.

Dentro del elemento negativo de este derecho se pueden encontrar elementos cautelares tradicionalmente conocidos como los "*principios de calidad de los datos*" (Garriga Domínguez, 2009, pág. 38). Dentro de estos principios se encuentran los siguientes:

- Principio de Pertinencia: El cual procura la pertinencia y congruencia de los datos personales con el fin perseguido, a la vez que procura la proporcionalidad de estos al establecer que dichos datos no deben ser excesivos en relación con su finalidad original. Ha sido tratado, entre otros autores, por Garriga Domínguez, Millán Salas & Peralta Ortega.
- Principio de Finalidad (o de Sujeción al Fin del Procesamiento): Procura que solamente puedan ser tratados y recogidos los datos personales adecuados al fin legítimo por el que fueron obtenidos originalmente, (para el cual el individuo ha brindado su consentimiento informado) y que por tal motivo, no puedan ser utilizados para otra finalidad a la originalmente planteada. Ha sido tratado, entre otros autores, por Hassemer & Chirino y Garriga Domínguez.
- Principio de Veracidad y de Exactitud: El cual *"exige que los datos sean exactos y estén actualizados de forma que respondan con veracidad a la situación del afectado"* (Garriga Domínguez, 2009, pág. 38).

- Principio de libertad de decisión individual: Busca asegurar al individuo su capacidad de decidir sobre "el fin u objetivo del procesamiento de sus datos personales" (Hassemer & Chirino, 1997, pág. 174).
- Principio de Lealtad: Procura la inexistencia de engaños o falsedades en el proceso de recolección de datos personales (Garriga Domínguez, 2009, pág. 38).
- Principio de Transparencia: Sumamente relacionado con el derecho a la información, este principio supera la mera necesidad de que el afectado conozca el tipo, dimensión y fin del tratamiento de sus datos personales, para incluir también la apertura necesaria del encargado al escrutinio sobre el tratamiento de los datos personales que lleva a cabo.

  Ha sido tratado, entre otros autores, por Hassemer & Chirino y Millán Salas & Peralta Ortega. Asimismo, es recogido como uno de los principios de la privacidad por diseño, a partir de la cual pueden darse incluso verificaciones de la seguridad de todas las etapas del tratamiento por entes independientes.
- Principio de Confidencialidad: Según Millán Salas & Peralta Ortega, establece la necesaria obligación de secreto que reside en quienes intervienen en el proceso de tratamiento de datos personales con respecto a su contenido.
- Principio de Seguridad de los Datos: Busca la adopción de las medias técnicas necesarias para garantizar que los datos personales tranzados no sufran alteraciones, pérdidas, tratamientos o accesos sin la autorización necesaria. Ha sido tratado, entre otros autores, por Garriga Domínguez, Millán Salas & Peralta Ortega.

- Principio de Separación de Poderes Informativos: Establece la necesidad de una correcta "división técnica y organizacional entre el procesamiento de datos frente a otros fines de utilización de los datos personales" (Hassemer & Chirino, 1997).[28]
- Principio de Prohibición de Procesamiento de Datos "a beneficio de inventario": Como su nombre lo establece, procura evitar que los datos personales sean recopilados sin mayor fin que el añadirlos a un inventario o a una base de datos, con tal de facilitar tratamientos de datos posteriores no autorizados, así como "la prohibición de la construcción de perfiles a partir del procesamiento de datos personales" (Hassemer & Chirino, 1997, pág. 38).
- Principio de aseguramiento técnico: Procura asegurar al individuo la certificación técnica[29] del cumplimiento de los principios jurídicos dirigidos a tutelar sus intereses y derechos frente al procesamiento de sus datos personales (Hassemer & Chirino, 1997, pág. 38).[30]
- Principio del control del procesamiento: Según Chirino busca asegurar el control del procesamiento de datos personales "a partir de lugares de procesamiento independientes" (Hassemer & Chirino, 1997, pág. 38)[31].

[28] En otras palabras, debe haber una división clara entre las funciones de tratamiento de datos de una empresa y aquellas ligadas, por ejemplo, con la publicación de la información. Esto con miras a asegurar que la información, por ejemplo.
[29] Por parte de un ente capaz de examinar dicho cumplimiento por medios técnicos especializados, como por ejemplo el ente regulador especializado o entes internacionales de estandarización.
[30] Por medio, por ejemplo, de la inclusión de personal técnico especializado en el proceso de aseguramiento de los datos.
[31] El cual procura extender las disposiciones del principio de separación de poderes informativos distanciando la ubicación geográfica de los centros de procesamiento de datos del lugar principal de trabajo de la empresa con miras a dificultar el acceso no autorizado a la información personal.

En segundo lugar, debe recordarse que los elementos positivos del derecho de autodeterminación informativa hacen referencia al conjunto de derechos subjetivos tutelados o agrupados dentro del habeas data, el cual se puede entender como una garantía procesal que busca asegurar al individuo su libertad positiva de supervisar el almacenamiento y uso de aquella información que le resulta relevante (Quesada Mora, 2004). Dentro de este conjunto de derechos se encuentran los siguientes:

- Derecho del titular de los datos a que se le informe de los bancos de datos existentes, de su titularidad y finalidad: Señalado por Garriga Domínguez y Murillo de la Cueva, este derecho se encuentra íntimamente relacionado con el derecho a la información, al requerir de todo ente que procese datos personales el informar previamente al interesado sobre los datos recabados, la identificación de quienes habrán de tratar tales datos y del fin para el cual serán tratados. Según Garriga Domínguez, de la existencia de una correcta información del individuo depende su capacidad de ejercer el derecho de autodeterminación informativa.
- Derecho del afectado a que se solicite su consentimiento para la recolección, tratamiento y cesión de sus datos personales: Comprende que de nada sirve informar al individuo del procesamiento de sus datos si no se solicita previamente al inicio de este su consentimiento. Evidentemente, la inexistencia de este consentimiento necesario torna ilegítimo todo tratamiento de datos personales.
- Derechos de acceso, rectificación y cancelación u oposición: Constituyen el núcleo de las potestades de actuación *a posteriori* tradicionalmente

reconocidas al individuo ante el tratamiento de sus datos personales. Implican la necesaria capacidad del individuo de acceder a todos los datos que sobre su persona existan en una base de datos; a rectificar aquellos que no sean actuales o que sean erróneos; y a exigir la eliminación de aquellos erróneos que se encuentren en la base de datos.

- Derecho al olvido: Procura la destrucción de los datos personales una vez cumplido el fin para el que fueran recabados, lo cual puede realizarse de oficio o a instancia del interesado. Usualmente las legislaciones establecen la obligación de llevarlo a cabo de forma oficiosa pasada cierta cantidad de tiempo, con miras a asegurar al interesado que deberá cargar en el futuro hasta por el más mínimo detalle de su pasado. Ha sido tratado, entre otros autores, por Garriga Domínguez, Murillo de la Cueva y especialmente por Peña Ortiz & Achío Gutiérrez en su tesis de grado.
- Derecho a no sufrir perjuicios como consecuencia de decisiones tomadas exclusivamente en virtud de perfiles personales obtenidos informáticamente (Murillo de la Cueva, 2007).
- Derecho a ser protegido por las instituciones especializadas creadas para defender este derecho (Murillo de la Cueva, 2007).

Se puede concluir ese apartado recordando a Quesada Mora, quien considera que estos principios pueden resumirse por buscar tres objetivos fundamentales, a saber:

*"a) Asegurar que los datos sean completos, actualizados y verdaderos, para lo cual se debe permitir las más amplias facilidades para rendir las pruebas que sean necesarias. No solo se afecta a la intimidad entrometiéndose en la vida de los otros, sino deformándola o falseándola*

*de modo de construir una imagen inexacta de la persona. b) Asegurar que el uso que se dé a los datos no desfigure o perjudique de modo alguno a quienes ellos se refieran (…) c) Asegurar que el uso de los bancos de datos no produzca una discriminación de los individuos a quienes la información se refiere"* (Quesada Mora, 2004).

## *Síntesis de la Segunda Sección*

Derecho a la Intimidad y el "Right to Privacy" Anglosajón

*A lo largo de la cual se definen las características y se detallan las diferencias existentes entre conceptos que hacen referencia a la protección de ámbitos privados de la personalidad individual pero responden a dos contextos legales distintos.*

El Derecho a la Intimidad

- No existe una definición unívoca de la totalidad de sus aplicaciones pues el contenido de este derecho ha variado a lo largo del tiempo, a pesar de lo cual puede comprenderse como *"el derecho que poseen las personas de poder excluir a las demás personas del conocimiento de su vida personal, es decir, de sus sentimientos y comportamientos" (Rojas Vega & Vargas Delgado, 2009, pág. 179).*
- Originalmente este derecho se encontraba limitado únicamente a la protección de la esfera más íntima del ciudadano, sin embargo en la actualidad se ha ampliado dicha protección a elementos de la vida privada de la persona que no necesariamente forman parte de la visión tradicional de la privacidad, por lo que sus características actuales incluyen las siguientes:
    - Abarca y protege tanto los ámbitos meramente individuales como los de su núcleo familiar.
    - Se trata de un derecho personalísimo.
    - Dota al sujeto de derechos de defensa (negativos) y de control (positivos), por lo que es un fundamento del derecho de autodeterminacion informativa.
    - Su protección recae tanto en el sujeto como en el Estado.
    - Garantiza un ámbito privado a la persona.
    - Es irrenunciable, imprescriptible, inalienable, intransmisible e inembargable.
- Los elementos fundamentales de ese derecho serán:

  - Vida Privada: Representa la necesidad de proteger los aspectos más íntimos de la personalidad humana y todos aquellos que no se consideran parte del ámbito público.
  - Privacidad: Representa las nuevas tendencias dirigidas a proteger incluso aquellos ámbitos (datos y metadatos) que parecieran ser irrelevantes pero que en su conjunto brindan una visión completa de la vida privada de un individuo.
  - Autonomía de la Voluntad: Se trata de *"la facultad de los particulares para regir y ordenar su propia conducta mediante sus propias normas sin depender de nadie ni ser obligado a ello por algún impulso externo" (Soro Russell, 2007, pág. 10).*

- No es posible identificar de manera precisa la distinción entre lo público y lo privado, por lo cual se ha dejado a la interpretación jurisprudencial determinar caso por caso el punto en que debe ubicarse tal distinción.
- Este derecho se encuentra limitado por el justo equilibrio entre los intereses individuales y generales. Específicamente en Costa Rica se encuentra limitado por la seguridad nacional, el bien común, el orden y seguridad pública, la salud o la moralidad pública y los derechos y libertades individuales.
- En el nivel nacional este derecho humano se encuentra protegido por el artículo 24 constitucional y ha sido abordado en múltiples ocasiones por la Sala Constitucional, la cual ha emitido votos representativos como los 1261-90, 5736-94 y 8022-99.
- En el nivel internacional este derecho humano se encuentra plasmado en instrumentos como la Declaración Universal de Derechos Humanos; el Convenio Europeo de Derechos Humanos; el Pacto Internacional de Derechos Económicos, Sociales y Culturales; el Pacto Internacional de Derechos Civiles y Políticos; y la Convención Americana sobre Derechos Humanos.

El Derecho a la Privacidad (el *"Right to Privacy"* Anglosajón)

- Es una creación del derecho anglosajón, por lo cual responde a un contexto legal distinto de aquel que genera nuestro derecho a la intimidad (Derecho Civil

o Continental). Encuentra sus orígenes en el artículo *"The Right to Privacy"* de Warren y Brandeis, quienes lo exploran como extensión del derecho a la propiedad privada.

- Se diferencia de nuestro derecho a la intimidad en tanto el derecho a la privacidad ha sido entendido por el derecho anglosajón desde sus inicios como una herramienta amplia que soporta el "*right to be left alone"* y ampara también a aquellos elementos de la personalidad que tradicionalmente superan la esfera *"más cercana al individuo"* que caracteriza a nuestro tradicionalmente limitado derecho a la intimidad.
- Su desarrollo por parte del derecho anglosajón resulta sumamente amplio, diversificándose su tratamiento a lo largo de las más variadas áreas del Derecho. A pesar de lo anterior es posible identificar cuatro clases fundamentales de ilícitos civiles concernientes a la privacidad:
    - Actos de intrusión que perturban el retiro o soledad del individuo: Los cuales afectan el derecho a permanecer voluntariamente aislado.
    - Divulgación pública de hechos privados embarazosos sobre el individuo: Que afectan su privacidad siempre y cuando no sean legítimamente concernientes al público.
    - Publicidad que coloca al individuo bajo una luz falsa ante el público.
    - Apropiación de la imagen o identidad de una persona para derivar algún beneficio.
- El derecho Constitucional estadounidense lo protege por medio de las enmiendas constitucionales Primera, Tercera y Cuarta, e igual protección ha sido generada por medio de gran cantidad de leyes aprobadas por el Congreso de los Estados Unidos (las cuales serán estudiadas más adelante).

<u>Derecho a la Información y Derecho de Autodeterminación Informativa</u>

*A lo largo de la cual se definen las características y se detallan las diferencias existentes entre dos derechos relacionados con el uso y manejo de la información por parte de entes públicos y privados y su relación con los individuos.*

El Derecho a la Información

- De carácter definitivamente multifacético, el derecho a la información se constituye en la actualidad tanto en estandarte de la libertad y dignidad individual y fundamento legitimador del uso individual de las nuevas tecnologías de la información y la comunicación; como en potencial amenaza a la dignidad humana, dada la posibilidad de su abuso en contra de la intimidad.
- Surgido a partir de las ideas de la Ilustración, es reconocido en la Declaración Universal de Derechos Humanos. Puede ser definido genéricamente como el derecho del individuo a *saber* y específicamente como aquella modalidad del derecho de petición que requiere la publicidad de los actos públicos y de la información que alcance el interés público (Córdoba Ortega, 1996, pág. 29).
- Una definición genérica del término *"información"* lo comprende como: *"la comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una determinada materia y emplea los procedimientos para acopiar, almacenar, tratar, difundir, recibir; así como los tipos, hechos, noticias, datos, opiniones, ideas y sus diversas funciones" (Valladares Lanza, 2008).*
- Frente al derecho a la información se debe subdividir la información en tres categorías:
    - Información Privada: Información protegida por los derechos de intimidad y privacidad.
    - Información Pública: Información perteneciente a todos los ciudadanos de una nación, en copropiedad, quienes pueden exigir el uso y disfrute de esta al Estado y sus entidades.
    - Información de Interés General: Información que a pesar de su carácter privado resulta relevante a los intereses de la comunidad, por lo que es trasladada de la esfera privada a la pública.
- Se trata de un derecho humano que puede ser comprendido como derecho subjetivo y como bien jurídico tutelado; sin embargo, su objeto (la información) *"no es universal, sino general, por lo que admite excepciones en la difundibilidad" (Villalobos Quirós, 1997, págs. 54-55).*
- Existen dos grupos de principios relevantes para este derecho, a saber:

  - Principios ideales (recomendados en el ámbito internacional): transparencia máxima; obligación de publicar; promoción del gobierno abierto; limitación a las excepciones; facilitación del acceso; disminución de costos; reuniones abiertas, precedencia de la transparencia; y protección para denunciantes.
  - Principios vigentes en el Derecho Administrativo costarricense: legalidad; transparencia administrativa; igualdad; publicidad; y democrático.
- Incluye conjuntos específicos para quien informa y quien es informado, a saber:
  - Quien informa: derecho a investigar; a emitir y difundir informaciones y opiniones por cualquier medio; a no ser censurado; a acceder a fuentes de información; al secreto profesional; a la cláusula de consciencia; y al acceso a los medios necesarios.
  - Quien es informado: a recibir opiniones e informaciones; a seleccionar la información y los medios; a recibir información veraz y oportuna, a que sea preservada su honra y vida privada; derecho de rectificación o respuesta; y derecho de acudir a los tribunales de justicia para exigir responsabilidad según dicta la ley.

El Derecho de Autodeterminación Informativa

- Profundamente arraigado en principios como la dignidad humana, la dignidad individual, a la autodeterminación y la democracia, este derecho humano es considerado como un derecho derivado de los derechos de intimidad, privacidad e información que adquiere una doble dimensión: sustancial (derecho en sí mismo) e instrumental (que soporta otros derechos).
- Puede afirmarse que el bien jurídico tutelado por este derecho es la libertad individual enfocada específicamente en el control de la información personal (datos y metadatos relativos a una persona). Esta tutela es facilitada por medio del establecimiento de una serie de garantías positivas (garantiza un haz de facultades, poderes y potestades para el control) y negativas (establece cautelas y límites al tratamiento).

- No se trata de brindar al individuo un poder absoluto e ilimitado sobre sus datos, pues sus límites se encontrarán marcados por el valor de la información como bien colectivo en el conjunto social. Según Hassemer & Chirino, estos límites serán legítimos en tanto satisfagan un interés público preponderante, tengan fundamento legal que cumpla con el principio de proporcionalidad y se basen en normas definidas y puestas en vigencia de manera clara y precisa (Hassemer & Chirino, 1997, pág. 177).
- Dentro de los elementos negativos de este derecho se pueden encontrar elementos cautelares conocidos como los *"principios de calidad de los datos",* dentro de los cuales están los principios de pertinencia; finalidad; veracidad y exactitud; libertad de decisión individual; lealtad; transparencia; confidencialidad; seguridad de los datos; separación de poderes informativos, prohibición de procesamiento de datos *"a beneficio de inventario";* de aseguramiento técnico; y de control del procesamiento.
- Por su parte, los elementos positivos de este derecho hacen referencia al conjunto de derechos subjetivos tutelados o agrupados dentro del habeas data, (garantía procesal que busca asegurar al individuo su libertad positiva de supervisar el almacenamiento y uso de su información), dentro de los que se encuentran: el derecho de información; de consentimiento informado; de acceso, rectificación y cancelación u oposición; al olvido; a no sufrir perjuicios y a ser protegido por las instituciones especializadas relevantes.

# Capítulo II: La Protección de Datos Personales, Evolución y Fundamentos Iusinformáticos Frente a la Convergencia de las Telecomunicaciones

El presente capítulo será dedicado al estudio de las características generales de la protección de datos personales en sus dos principales vertientes: jurídica e informática. Por ello, a lo largo del apartado se abarcarán cuatro aspectos fundamentales: los elementos históricos que marcaron el surgimiento de la protección de datos; la realización de una breve tipología de los datos en cuestión; los fundamentos técnicos y jurídicos que posibilitan la protección de datos; y la problemática que rodea al el tema en el mundo moderno.

## Sección I: Surgimiento y Fundamentos de la Protección de los Datos Personales desde la Perspectiva Iusinformática

Esta sección se dedicará al estudio de la evolución, los fundamentos y la problemática relacionada con la protección de datos personales desde la perspectiva iusinformática. Para lograr tal fin, se iniciará con un breve recuento histórico del surgimiento de la perspectiva iusinformática en paralelo con la evolución de las tecnologías de la información y la comunicación.

Seguidamente, se realizará una breve caracterización de la protección de datos desde la perspectiva iusinformática y se estudiarán sus objetivos, sujeto y objeto (señalando una breve tipología de los tipos de datos que conforman dicho objeto), y se culminará con la determinación de los principios relevantes para la protección de datos y su aplicación en las diversas etapas de esta.

## *Surgimiento de la Perspectiva Iusniformática: el Derecho Informático y los Orígenes de la Protección de Datos*

### Breve Introducción Histórica y Contextual

#### *El Surgimiento de las Bases de Datos*

Según Beunen, se puede definir una base de datos como una *"colección de trabajos independientes, datos u otros materiales acomodados de manera sistemática o metódica e individualmente accesible por medios electrónicos o por otros medios"* (Beunen, 2007, pág. 21). Asimismo, señala la autora que, de conformidad con el uso comúnmente brindado al término, el Oxford English Dictionary describe una base de datos como *"una colección estructurada de datos mantenida en almacenamiento informático; especialmente en aquel que incorpora software para hacerla accesible en una variedad de formas"* (Beunen, 2007, pág. 21).

Es bien sabido que los seres humanos han almacenado información desde el inicio de la historia. Las primeras bases de datos creadas tendían a ordenar dicha información de manera útil mediante principios prácticos que, con el paso del tiempo, fueron adquiriendo mayor complejidad.

Estos principios han sido aplicados al manejo de información por parte de entes privados y públicos por igual, los cuales se han visto en la necesidad de manejar grandes cantidades de información sobre los más diversos temas (Intuit Inc., 2013). Para tal fin, el surgimiento de la informática implicó una verdadera revolución al posibilitar el tratamiento, manipulación, acumulación y elaboración de datos,

mediante la configuración de los sistemas de cómputo como sistemas automatizados de administración de bases de datos.

El principal precursor de un sistema automatizado dirigido al tratamiento y almacenamiento de información personal data del año de 1884, con la creación de la *máquina tabuladora*[32] por Hernman Hollerith, con lo cual revolucionó el análisis de la información del censo, al desarrollar un sistema capaz de clasificar la información según criterios como sexo, etnia, estado civil y edad (Garriga Domínguez, 2010).

La historia de los sistemas automatizados de administración de bases de datos da inicio durante la década de los años 60, en la cual la disminución de los precios de los sistemas computacionales permitió que tanto entes públicos como privados adquirieran y establecieran sus propias bases de datos, las cuales fueron utilizadas, entre otros fines, para el manejo de información concerniente a individuos[33].

La década de los años 70 se vio marcada por un cambio en el sistema organizacional utilizado por el común de la industria en sus bases de datos, cuando E.F. Codd propone el paso de un modelo de bases de datos jerárquicas[34] a un modelo de bases de datos

[32] Al respecto de las cuales Black y Garriga Domínguez, afirman que "La máquinas diseñadas por Hollerith fueron utilizadas por los nazis en Alemania para elaborar el censo de 1933. El uso de las tarjetas perforadas permitió elaborar una ficha informatizada de cada persona internada en los campos de exterminio. A cada categoría de personas, se le asignaron determinados códigos numéricos en las tarjetas perforadas. Había hasta 16 categorías diferentes que se clasificaban en función de los agujeros de las tarjetas: el agujero 3 significaba homosexual, el 9 antisocial, el 12 gitano y el número 8 judío. Sin duda, el uso de las tarjetas perforadas fue de suma utilidad para la localización y clasificación de los grupos de personas que posteriormente serían víctimas del genocidio nazi." (Garriga Domínguez, 2010, pág. 1); lo cual sin duda alguna constituye uno de los ejemplos más tempranos de tratamiento automatizado de datos personales con fines abusivos llevado a cabo por un ente estatal.

[33] Ejemplo de lo cual se puede encontrar en el sistema SABRE utilizado por IBM para ayudar a American Airlines a manejar las reservaciones aéreas (Intuit Inc., 2013).

[34] En el que la información es organizada utilizando una estructura similar a la de un árbol genealógico, lo que permite representar las relaciones existentes entre la información usando relaciones que permitían determinar los atributos de un dato específico. Ver ejemplo en Anexo 1.

relacionales[35]; esto permite desconectar el modelo lógico de la base de datos del almacenamiento físico de la información (Intuit Inc., 2013), agilizar la evolución de las bases de datos y facilitar nuevos y más eficaces métodos de búsqueda de información. Este modelo pronto es adoptado como el principal estándar aplicado en la industria de bases de datos y obtiene especial éxito a lo largo de la década de los años 80.

La década de los años 90 ve nacer herramientas dirigidas a facilitar la creación de bases de datos personales tales como Excel y Access. El posterior advenimiento del internet conlleva a una explosión de la industria de las bases de datos, la cual comienza a implementar sistemas de acceso a bases de datos principales (cliente-servidor), que posibilitan a los usuarios de computadoras de escritorio convencionales el almacenamiento de grandes cantidades de información histórica pese a las limitaciones de los sistemas de escritorio del momento (Intuit Inc., 2013).

El gigantesco empuje de inversión en el internet que caracterizó los últimos años de la década de los 90, implica el incremento en la demanda por sistemas de manejo de bases de datos con conectividad con la red de redes. Asimismo, durante esta época surge la demanda por sistemas capaces de procesar transacciones en línea y el procesamiento analítico de datos (Intuit Inc., 2013), que permitiera analizar grandes cantidades de datos desde múltiples perspectivas conformes con las necesidades del negocio.

Finalmente, la década del 2000 ve surgir las novedosas aplicaciones posibles de las bases de datos, extendiéndose su uso a las nuevas tecnologías móviles, así como a las

[35] En el que todos los datos poseen un número identificador que les permite interrelacionarse y establecer sus atributos de manera más eficiente. Ver ejemplo en Anexo 2.

tecnologías "en la nube"[36]; las cuales, no solamente garantizan la resiliencia de los datos, sino que también permiten su disponibilidad inmediata y el acceso ubicuo a dicha información. Asimismo, en tanto la primera década del siglo XXI significó el surgimiento de técnicas y tecnologías que posibilitaron el análisis de gigantescas cantidades de información en poco tiempo, es común en la actualidad encontrar menciones a la existencia de extensos sistemas dedicados al tratamiento de datos personales de los usuarios del internet, con los más diversos fines.

### *Las Técnicas de Seguridad de la Información*

En los inicios de la era de la computación, la única manera existente de compartir información entre dos computadoras centrales *("mainframes")* era el envío por medios físicos de dicha información (envío por correo u otros medios, de las cintas magnéticas que contenían la información). Esta situación implicó que las técnicas de seguridad de la información durante esta época se basaran simplemente en garantizar la seguridad física de las computadoras centrales (mainframes) y los medios de almacenamiento de información utilizados (Lewis University, 2013).

En la década de 1960 el contexto mundial, caracterizado por la Guerra Fría y la expansión militar, causó un aumento significativo en la cantidad de computadoras existentes en el mundo. Estas computadoras requerían, para mantener su eficiencia con respecto a los costos, el ser utilizadas de manera continua (Global Data Vault,

[36] Tecnología que permite que los procesos computacionales sean realizados en un sitio remoto e indeterminado por medio del Internet. "La nube es un sistema computacional inteligente, complejo y poderoso en el cielo, al cual la gente simplemente se conecta" (Hamm, 2008).

2012) y el trabajo realizado por ellas comenzó a requerir que el procesamiento y almacenamiento de los datos se realizara de manera descentralizada (Lewis University, 2013).

Esta situación llevó al Departamento de Defensa estadounidense a la creación de la ARPANET, con miras al establecimiento de una red redundante y confiable mediante la cual las diversas computadoras centrales existentes pudieran transmitirse mutuamente información en tiempo real.

La creación de una red a gran escala dirigida al manejo de información de alta prioridad, tuvo como consecuencia el fin de la época en la que la seguridad de la información se relacionaba solamente con la seguridad física. La existencia de problemas de seguridad debidos a la falta de estandarización en los métodos de protección de las bases de datos en los diversos centros, se hizo evidente conforme pasó el tiempo.

Ante esta realidad, los esfuerzos por reforzar la seguridad de los sistemas informáticos no se hicieron esperar. A principios de la década de 1970, el Departamento de Defensa estadounidense publicó un reporte titulado "*Security Controls for Computer Systems*" que actualmente es considerado por muchos académicos como el *"trabajo seminal en el estudio de la seguridad informática, dado que explícitamente llamó a alejarse de la concepción de la seguridad informática vinculada puramente la protección del hardware hacia su concepción en términos de datos, usuarios e infraestructura. Llamó al reconocimiento de que los datos son la mercancía de interés, que las credenciales de los usuarios deben ser confiablemente verificadas para mantener segura esa mercancía, y que asegurar que esto se*

*realice correctamente no requiere de reacciones ad-hoc, sino de un plan institucional comprehensivo y de múltiples niveles"* (Lewis University, 2013).

Los cambios impulsados por el informe se unieron con una multitud de proyectos surgidos a partir de la popularización de la computación personal y el surgimiento del Internet durante la década de 1980. Nuevas técnicas de seguridad de la información surgieron durante esta época en respuesta a los siempre crecientes retos, a la vez que dio inicio un proceso de estandarización de los principios necesarios para garantizar la seguridad de la información en este nuevo mundo.

Actualmente, la seguridad de la información se encuentra regida por tres principios fundamentales: confidencialidad[37] (la prevención de la liberación de la información a entes o sistemas no autorizados), integridad[38] (que procura evitar cambios no autorizados en la información a la vez que busca el mantenimiento de la precisión y la consistencia de la información a lo largo de su ciclo de vida) y disponibilidad[39] (el asegurar que la información se encuentre disponible siempre que esta sea requerida).

A partir de esta triada de principios, entes internacionales como la Organización para la Cooperación y el Desarrollo Económico (OCDE), el Instituto Nacional de Estándares y Tecnología (NIST) estadounidense y la Sociedad del Internet[40] han establecido una cantidad cada vez mayor de principios relacionados con la seguridad de la información,

[37] Definida como: "La calidad o estado de la información que previene su revelación o exposición a individuos o sistemas no autorizados" (Whitman & Mattford, 2012, pág. 583)
[38] Definida como: "La calidad o estado de encontrarse enero, completo e incorrupto" (Whitman & Mattford, 2012, pág. 589)
[39] Definida como: "Una calidad o estado de la información caracterizada por encontrarse accesible y correctamente formateada para su uso sin interferencia u obstrucción" (Whitman & Mattford, 2012, pág. 580)
[40] Por medio de grupos de trabajo y estandarización tales como la Internet Engineering Task Force.

tales como los principios de *autenticidad*[41] *y no repudio*[42], los nueve principios establecidos por la OCDE en su Guía para la Seguridad de los Sistemas de la Información y las Redes (Organización para la Cooperación y el Desarrollo Económico, 2002) y los 33 principios establecidos por la NIST para la seguridad de las tecnologías de la información (Stonebruner, Hayden, & Feringa, 2004).

Actualmente es posible encontrar desde directrices dirigidas a garantizar la seguridad de la información y su contexto social[43]; hasta estándares técnicos enfocados en la práctica[44]. Así, se pueden caracterizar las técnicas de seguridad de la información por requerir que los controladores de la información adopten una perspectiva holística en materia de seguridad, en la cual tomen en consideración la totalidad del entorno (contexto, disposiciones internas, directrices legales y estándares técnicos) de la información protegida.

Tal protección es llevada a cabo actualmente mediante la implementación de procesos de "defensa en profundidad" de la información, que procuran identificar y proteger los

[41] Definida como: "Una calidad o estado de la información caracterizada por ser genuina u original antes que reproducida o fabricada" (Whitman & Mattford, 2012, pág. 580).
[42] Definido como: "El principio de criptografía que da crédito al mecanismo de autenticación colectivamente conocido como una firma digital. En este proceso criptográfico asimétrico, la llave privada del remitente es utilizada para encriptar un mensaje, y la llave pública del remitente debe ser utilizada para desencriptar el mensaje –cuando la desencriptación ocurre correctamente, provee verificación de que el mensaje fue enviado por el remitente, lo cual no puede ser refutado" (Whitman & Mattford, 2012, pág. 591).
[43] Como es el caso de los principios de la OCDE, los cuales tocan temas como la concienciación, la responsabilidad, la respuesta, la ética, la democracia, la evaluación del riesgo, el diseño y realización de la seguridad, la gestión de la seguridad y la reevaluación. (Organización para la Cooperación y el Desarrollo Económico, 2002, págs. 8-9)
[44] Como es el caso de los estándares Técnicos de la NIST y demás entes generadores de estándares, los cuales usualmente tocan temas como los controles administrativos, locales y físicos de la información; la clasificación y el control de acceso de la información; los métodos criptográficos a utilizar; la gobernanza de la seguridad y el establecimiento de planes de respuesta; y el planeamiento de planes de recuperación ante desastres.

elementos que conforman los sistemas de información (capas física, de red, de infraestructura, de aplicaciones y de datos).

El primer elemento por proteger es la capa física (Programa Sociedad de la Información y el Conocimiento, 2010, pág. 240) de los sistemas que almacenan los datos. Este elemento se preocupa por el aseguramiento constante y redundante de la infraestructura física que soporta el sistema de información por medio de la implementación de protocolos relacionados con manejo de emergencias (suministro eléctrico, protección contra incendios y otros), seguridad física del establecimiento (cámaras y alarmas de seguridad, patrullaje, protocolos de acceso y otros).

La segunda capa por proteger es la infraestructura (Programa Sociedad de la Información y el Conocimiento, 2010, pág. 240) que conecta el sistema de información con el exterior: las redes internas y externas. Este segundo elemento se encuentra conformado fundamentalmente por instrumentos dirigidos a prevenir ataques virtuales a la información, lo cual es realizado mediante la implementación de elementos de hardware y software que permiten detectar ataques y responder automáticamente a ellos (sistemas de detección de intrusiones y sistemas de prevención de intrusiones) o que se dedican a separar sectores de la red interna para evitar su fácil acceso (*switches)* o a la revisión y filtrado constante de los paquetes de datos entrantes y salientes (*Firewalls).*

En la protección de la tercera capa, referente a la infraestructura real del sistema de información (Programa Sociedad de la Información y el Conocimiento, 2010, pág. 241) deben ser identificados todos los elementos que componen el sistema propiamente

dicho (servidores, computadoras, periféricos, sistemas operativos, entre otros) con miras a garantizar que estos reciban mantenimiento adecuado (tanto físico como digital mediante el parcheo del software y la revisión del estado físico del hardware involucrado).

La cuarta etapa que debe seguirse en un proceso de aseguramiento de la información se dirige al control de las aplicaciones o paquetes de software involucrados en el tratamiento de la información. Para ello resulta de fundamental importancia el establecer un orden de desarrollo de las aplicaciones, el control de la salida y la entrada de datos, la separación de labores (desarrolladores de las aplicaciones, prueba de estas, administración de las bases de datos, entre otros) y el establecimiento de controles de acceso a la información que permitan la identificación de los usuarios y los privilegios que posee cada uno de ellos (Programa Sociedad de la Información y el Conocimiento, 2010, pág. 242).

Por último, los procesos de defensa en profundidad de la información se dedican al establecimiento de protocolos y la implementación de medidas dirigidas a asegurar los datos frente a los múltiples peligros que les asechan. En esta etapa, la protección se centra fundamentalmente en el establecimiento de sistemas de protección redundante de los datos (sistemas en los cuales nunca existe una sola copia de los datos, sino que existen múltiples copias) y el uso de métodos de encriptación de los datos, los cuales aseguren que la información contenida en el sistema no pueda ser utilizada en caso de ser sustraída (Programa Sociedad de la Información y el Conocimiento, 2010, pág. 242).

Las técnicas de defensa de la información han logrado evolucionar y superar las perspectivas cerradas de defensa de los elementos tangibles de los sistemas informáticos que las caracterizaban inicialmente. En su refinamiento, han adquirido también un carácter mucho más amplio y consciente de su contexto, una visión holística, que ha posibilitado la generación de principios técnicos y legales, que adquieren gran importancia en los actuales sistemas de protección de datos personales.

### *El Derecho Informático y la Perspectiva Iusinformática*

Tal como se estudió en la sección primera del capítulo primero, la segunda mitad del siglo XX se ve marcada por la rápida evolución de las tecnologías de la información y la comunicación. El advenimiento de estas nuevas tecnologías supone, para el panorama cultural humano, la apertura de las fronteras electrónicas como nuevo medio de información capaz de superar las limitaciones de los medios de transmisión de conocimientos tradicionales (imprenta, transmisión oral y otros).

Este nuevo panorama cultural, se define según el profesor Ethain Katsh, como una verdadera "cultura electrónica", en la cual se tornan fundamentales *"las nuevas tecnologías de la información (TI), que (…) constituyen nuevas formas de recibir y transmitir información de forma más interactiva y permite(n) recoger, seleccionar, organizar, almacenar y transferir cualquier cantidad de información de un sitio a otro, sin fronteras, a velocidades y formatos electrónicos"* y que, *"marcan nuevos derroteros y formas diferentes de regular la vida social, política, cultural, científica del hombre" (Riascos Gómez, 1999).*

La cultura electrónica implica, para el mundo de finales del siglo XX, el inicio de un importante cambio de paradigmas, en el cual se vuelve cada vez más trivial la comunicación a escala global y la adopción a gran escala de medios informáticos o electromagnéticos de recopilación, selección, organización, almacenaje y transferencia de información. Las consecuencias de dicho cambio han afectado todos los sectores del saber humano (incluido, por supuesto el Derecho), así como los ámbitos que conforman las relaciones interpersonales e incluso las interestatales.

Al respecto, Riascos Gómez afirma que la cultura electrónica implica la creación de *"nuevos espacios, que desafían abiertamente los actuales límites geográficos de los estados, que plantean nuevos modelos de autoridad dentro conceptos [sic] diferentes a los que se tiene de la soberanía en los mapas y divisiones geopolíticas de hoy"* en los que se ha *"potenciado el manejo de la información activa y pasiva de tipo textual, visual o auditiva con tratamientos, procedimientos y formatos estrictamente electrónicos, a tal punto que hoy podemos hablar de una comunicación dinámica o electrónica que como surtidor genera una nueva visión de la vida personal, social, política y científica"* (Riascos Gómez, 1999).

Ante esta realidad surgen nuevas disciplinas dentro del Derecho, tales como la "Informática Jurídica" [45], el "Derecho de la informática" [46] y el Derecho del ciberespacio[47]. Estas disciplinas se encuentran dirigidas al estudio de la problemática

[45] Definido por Suñé Lliñás como *"la aplicación de los ordenadores electrónicos orientada a la resolución de problemas jurídicos o, cuando menos, de problemas específicos de los profesionales del Derecho"* (Suñé Llinás, 2006, pág. 8) tales como la gestión y soporte ofimático de las oficinas y despachos, la creación de bases de datos especializadas y la creación de sistemas de inteligencia artificial que buscan facilitar la toma de decisiones dentro del Derecho.

[46] Definida por Suñé Lliñás como el "conjunto de normas reguladoras de objetos teleinformáticos o de problemas directamente relacionados con la teleinformática" (Suñé Llinás, 2006, pág. 7).

[47] Que busca discernir las maneras en que el Ciberespacio debe (o no) ser regulado por el derecho. El término *"Ciberespacio"* fue originalmente acuñado por el escritor de ciencia ficción William Gibson en 1984 en su novela "Neuromancer", en la cual lo define como *"Una alucinación colectiva experimentada diariamente por miles de millones de operadores de computadores en cada nación… una representación*

planteada por las tecnologías de la información y la comunicación, así como el particular panorama que representa la existencia de un "metaespacio" (ciberespacio) facilitado por las redes informáticas que escapa tanto de los ámbitos tradicionales del Derecho estatal, como del control del Derecho Internacional.

El paso del tiempo, aunado con la convergencia de las nuevas tecnologías en la realidad resulta de esta manera en el surgimiento de nuevas vertientes del Derecho relacionadas con las tecnologías de la información y la comunicación. Así, partiendo desde 1949 se ha escuchado hablar de términos relacionados con la informática jurídica como la "*Jurimetría*"[48] *y la "Juritécnica*"[49]; y de campos de estudio como la *contratación electrónica*[50]*, comercio electrónico*[51], la *ciberseguridad*[52], la protección de

*gráfica de los datos resumidos de los bancos de cada computador en los sistemas humanos. Una complejidad inconcebible. Un variado grupo de constelaciones de datos vuela sin espacio en la mente, Las ciudades se iluminan recibiéndolos"* y en el que "la cultura se orienta alrededor de información en forma digital en lugar de la información impresa" - Ethain Katsh citado por (Riascos Gómez, 1999).

[48] La cual se centra en la posibilidad de buscar la manera de aplicar el procedimiento lógico, racional y automatizado posibilitado por las nuevas tecnologías como método de solución de controversias. La idea como mencionamos arriba fue ideada por el abogado norteamericano Lee Loeviner, para más adelante ser retomada por el inglés Hans Baade y refutada por el juez norteamericano Wesley Hohfeld (Riascos Gómez, 1999).

[49] Término acuñado por Vittorio Frosini que procura superar las limitaciones prácticas de la Jurimetría pensando en la informática como un medio auxiliar al derecho y no como un medio determinante en la toma de decisiones.

[50] Definido como *"Todo proceso de formación de un contrato que involucre exclusivamente el uso de medios electrónicos. Un contrato será el resultado de dicho proceso, cuando se plasme exclusivamente en un medio electrónico" (Rincón Cárdenas, 2006, pág. 53).*

[51] El cual consiste en *"realizar electrónicamente transacciones comerciales; es cualquier actividad en la que las empresas y consumidores interactúan y hacen negocios entre sí o con las administraciones por medios electrónicos" (Comisión de las Comunidades Europeas, 1997, págs. 7-10)*.

[52] Según la Unión Internacional de Telecomunicaciones, es el *"conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad."* (Unión Internacional de Telecomunicaciones, 2010).

datos personales, la gobernanza de internet[53] y el gobierno electrónico[54], entre otros, que finalmente se unen bajo el auspicio de su propia rama del Derecho: el Derecho Informático.

Esta nueva rama del Derecho, surgida en los años setenta presenta, un *"fundamento teórico, método y procedimientos propios"* (Riascos Gómez, 1999) y que *"… considera a la informática como instrumento (Informática Jurídica) y objeto de estudio (Derecho de la* Informática)" (Téllez Valdés, 2003, pág. 6), por lo que las incluye al constituirse en la rama de las ciencias jurídicas que estudia *"el conjunto de normas que dentro de un determinado sistema jurídico, regulan los procesos de información"* (Pérez Luño, Soriano Díaz, & Gómez Torres, 2004).

Confrontados con un nuevo y siempre cambiante campo de estudio, los profesionales en Derecho Informático deben dejar de lado la visión tradicional del Derecho y se ven forzados a encontrar por sus propios medios una síntesis entre los conocimientos técnicos especializados de la ingeniería informática y la visión legal de la problemática. De este esfuerzo aún vigente surge la perspectiva iusinformática, que procura adoptar un punto de vista holístico e interdisciplinario para solventar de formas creativas los problemas surgidos a partir de las nuevas tecnologías.

[53] Definida como *"el desarrollo y la aplicación por los gobiernos, el sector privado, y la sociedad civil, en las funciones que les competen respectivamente, de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y utilización de Internet" (Pérez & Ramos, 2007, pág. 2).*

[54] Que puede ser entendido como *"el uso de las Tecnologías de Información y Comunicación TIC, por parte de las instituciones de gobierno, para mejorar cualitativamente los servicios e información que se ofrecen a los ciudadanos; aumentar la eficiencia y eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación ciudadana" (Organización de los Estados Americanos, 2008).*

*Adopción Legal de la Protección de Datos Personales*

Tal como se estudiara anteriormente, las décadas de 1960 y 1970 resultaron de especial importancia para el desarrollo de las tecnologías de la información. El acelerado progreso en el campo del procesamiento electrónico de datos y la aparición de computadores centrales de bajo costo permitieron tanto a las administraciones públicas como a las grandes empresas el crear sus propias bases de datos dirigidas, entre otros fines, a recolectar, almacenar, tratar y transmitir información personal.

Más aún, tal como lo establece Pérez Luño, *"Desde los años setenta es notorio que bancos de datos del sector público norteamericano, pertenecientes al Pentágono, la CIA o el FBI, procesan informes sobre actitudes individuales y comportamiento político que afectan a millones de ciudadanos. Datos que recabados en función de la defensa nacional o de la seguridad pública han servido en determinadas ocasiones, para prácticas de control político y discriminación ideológica"* [55] (Pérez Luño A. , 2000, pág. 60).

Esta situación, aunada con las nuevas tendencias dirigidas a posibilitar el procesamiento de información a escala global por medio de las redes de telecomunicaciones y la inexistencia en ese tiempo de técnicas adecuadas de seguridad de la información, llamó la atención de las autoridades europeas, tanto

[55] Al respecto, el autor recuerda los ejemplos estadounidenses de universidades que entregaban información exhaustiva a la policía de aquellos alumnos y profesores sospechosos de ser contestatarios o disidentes y las aún existentes agencias de información comercial y de crédito que almacenan datos personales concernientes a cientos de millones de individuos a nivel global y que son transmisibles (a cambio de una compensación económica sustancial) organizados en más de 10000 maneras.
Asimismo, se encuentra un importante precedente en Francia, donde el Instituto Nacional de Estadística pretendía implementar un sistema de identificación único ante la administración (cuyas siglas curiosamente respondían a la palabra "SAFARI") el cual causó revuelo al llamar la atención sobre el peligro del cruce de ficheros y la formación de perfiles personales (Pérez Luño A. , 2000, pág. 61).

nacionales como internacionales, hacia la potencial vulnerabilidad de la información personal y las consecuencias que dicho tratamiento podría implicar para la privacidad e intimidad de los individuos (Rudgard, 2012, pág. 3).

Tal como asegura Rodotà, *"Para comprender el presente, y mirar al futuro, es indispensable ser conscientes del pasado"* (Rodotà, 2006, pág. 54). Con tal fin, debe recordarse fundamentalmente que los orígenes de la normativa actual sobre protección de datos pueden ser encontrados *"en el artículo 12 de la Declaración de Derechos Humanos de 1948, el cual establece la protección contra la injerencia arbitraria en la vida privada, así como el derecho a la libertad de opinión y expresión que incluye el derecho a no ser molestado a causa de las opiniones (art. 19)"* (Prieto Gutiérrez & Moreno Cámara, 2006, pág. 4).

Tomando tal derecho humano en consideración, desde 1968 se forma en el seno del Consejo de Europa una Comisión Consultiva con el fin específico de *"estudiar la incidencia sobre la intimidad que podría tener el tratamiento de datos de carácter personal mediante técnicas informáticas"* (Davara Rodríguez, 2006, pág. 28), consecuencia de la cual fue promulgada la Recomendación 509 del Consejo de Europa sobre *"los derechos humanos y los nuevos logros científicos y técnicos"* y que se constituye, según Puente de la Mora, en el *"origen de lo que posteriormente se le conoce como protección de datos personales" (Puente de la Mora, 2010, pág. 912)*.

El artículo 8 de la Recomendación establecía la necesidad de que se estudiara la situación de los países miembros, con miras a discernir si sus legislaciones nacionales protegían *"adecuadamente el derecho a la privacidad contra violaciones que puedan ser cometidas mediante el uso de métodos técnicos y científicos modernos"* (Consejo de Europa, 1968, pág. 1). A partir de la afortunada coincidencia de las propuestas de la

Recomendación con los diversos procesos legislativos nacionales, da inicio en Europa el proceso de generación legislativa en materia de protección de datos.

Antes de entrar con profundidad en el estudio de las características de este primer esfuerzo legislativo, debe recordarse la opinión de Pérez Luño, quien establece en su texto una clasificación generacional de las leyes de protección de datos. Debido a que nadie puede explicar mejor que dicho autor las características de esta clasificación, a continuación se citarán sus palabras:

*"Si la informática y las libertades han evolucionado generacionalmente nada tiene de particular que el punto de encuentro entre ambas categorías, es decir, la libertad informática responda a su vez, a una decantación generacional. En efecto, la experiencia legislativa de estos últimos años registra una sucesiva decantación desde las leyes de la primera generación, basadas en la autorización previa de los bancos de datos en una etapa en la que los equipos informáticos eran escasos, voluminosos y fácilmente localizables; a las leyes de la segunda generación, cuyo principal objetivo fue garantía de los datos "sensibles" por su inmediata incidencia en la privacidad o su riesgo para prácticas discriminatorias; y, en la actualidad, a las de la tercera generación, que se han hecho cargo de la revolución microinformática con la consiguiente difusión capilar de los bancos de datos. Ello ha hecho prácticamente inviable el control previo de los equipos informáticos, sobre el que operaron las normas de la primera generación; al tiempo que la tutela de las informaciones ya no puede quedar circunscrita al factor estático de su calidad, según el criterio predominante en la segunda generación de leyes de protección de datos, sino que debe hacerse extensiva a la dinámica de su uso o funcionalidad"* (Pérez Luño A. , 2000, págs. 63-64).

Siguiendo la clasificación establecida por Pérez Luño, y recordando también las opiniones de Chirino, Solorio Pérez (Solorio Pérez, 2009, pág. 2) y Puente de la Mora,

puede afirmarse que, dentro de la primera generación de leyes de protección de datos, es en el *Land* alemán de Hesse donde se promulga la primera norma vinculante sobre el tema el 7 de octubre de 1970.

El ejemplo alemán fue posteriormente seguido por el parlamento sueco el 11 de mayo de 1973, al establecer una ley dirigida a la protección de bases de datos, tanto públicas como privadas, el establecimiento de principios de protección de la información y la creación de *"la primera autoridad específica en la materia"* (Puente de la Mora, 2010, pág. 912). Asimismo, señala Puente de la Mora que forma parte de esta primera generación la *Privacy Act* estadounidense de 1974, a pesar de que esta solamente estableció la protección de las bases de datos públicas.

La segunda generación de leyes sobre protección de datos procura la protección de la información personal, para lo cual brinda especial importancia a los llamados *"datos sensibles". D*entro de esta generación de leyes se encuentran las creadas entre 1977 y 1979 por las repúblicas de Alemania, Francia, Dinamarca, Austria y Luxemburgo (Puente de la Mora, 2010, pág. 912).

Finalmente, los autores consideran que las leyes sobre el tema alcanzan su madurez a partir de la década de 1980, cuando los elementos de la protección de datos comienzan a ser reconocidos como derechos ciudadanos[56], a la vez que comienzan a ser reguladas algunas medidas técnicas de seguridad dentro de ellas. Dentro de los países que aprueban legislación sobre protección de datos en esta época están: *"Suiza*

[56] "*La autodeterminación informativa fue reconocida como derecho fundamental por parte del Bundesverfassungsgericht en 1983"* (Rodotà, 2006, pág. 54).

*(1981), Gran Bretaña (1984), Finlandia (1987), Holanda (1988), Islandia (1989), Alemania unificada (1990), Portugal (1991) y España (1992"* (Puente de la Mora, 2010, pág. 913).

Esta tercera generación culmina en 1998 cuando dan inicio los procesos de unificación de las leyes de protección de datos, por medio de la cooperación de los Estados miembros de la Unión con algunos Estados externos al régimen comunitario Europeo, por medio de mecanismos como la ratificación de "niveles de protección equiparable" y el establecimiento de sistemas de "*Safe Harbor*" como el existente entre Estados Unidos de América y la Unión Europea.

Esta situación sirve de antecedente inmediato a la situación actual de los regímenes legales internacionales sobre protección de datos[57] (los cuales se estudiarán con mayor detenimiento a lo largo del capítulo tercero de la presente investigación), en la cual la autodeterminación informativa comienza a ser considerada como un derecho humano del nivel internacional y en la que la materia supera indudablemente el "*sector del mercado interno al de la libertad, seguridad y justicia, con un explícito reconocimiento del hecho de que nos encontramos en este momento frente a una materia irreducible únicamente a la lógica económica, ya que toca derechos y libertades de las personas"* (Rodotà, 2006, pág. 54).

## Caracterización de la Protección de Datos desde la Perspectiva Iusinformática

[57] Dentro de los cuales se pueden encontrar algunos ejemplos capaces de ser calificados como parte de una cuarta generación preocupada por la cooperación internacional en protección de datos personales. Estos ejemplos de normativa internacional apuntan hacia la interoperabilidad y la responsabilidad como soluciones regionales o globales, a la problemática causada por el carácter transnacional de las telecomunicaciones convergentes.

*Definición Terminológica*

La protección de datos ha sido usualmente confundida con el habeas data (e incluso con la autodeterminación informativa) por parte de la doctrina jurídica estudiada, la cual se basa usualmente en el marco regulatorio vigente para determinar el término por utilizar, sin prestar demasiada atención a los detalles conceptuales. A pesar de tal situación, se hace necesario presentar al lector una precisión terminológica que permita adentrarse con mayor claridad en el tema.

Para los efectos de la presente investigación, debe considerarse primeramente que el concepto de *autodeterminación informativa* hace referencia al derecho humano anteriormente estudiado, el cual se caracteriza por subsumir los principios del derecho de la intimidad dentro del marco contextual de la sociedad de la información y la comunicación, a la vez que aboga por su comunicación y coexistencia con otros derechos aparentemente contrapuestos a la intimidad, tal como el derecho a la información.

Dentro de las múltiples soluciones que los diversos sistemas legislativos han encontrado para la problemática planteada por el derecho de autodeterminación informativa, el habeas data hace referencia a una garantía procesal que, tal como se estudiará más adelante, ha sido acogida por algunos de los países que han optado por asegurar la protección de tal derecho desde el ámbito constitucional.

Finalmente, el concepto de "*protección de datos*" hace referencia a un conjunto de técnicas y herramientas, iusinformáticas que buscan asegurar la salvaguarda de los datos a lo largo de su necesario manejo en la sociedad de la información y la

comunicación. Las instituciones jurídicas y herramientas técnicas de protección de datos personales se enfocan en estos y buscan garantizar al individuo la protección de su personalidad virtual (y consecuentemente, de su autodeterminación informativa) en un mundo que comprenden como intrínsecamente interconectado y caracterizado por el continuo proceso de creación, tratamiento y transmisión de información en el ámbito global.

Surge un concepto iusinformático cuya existencia y comprensión se tornan necesarias, tanto en la órbita jurídica de todas las ramas del Derecho; como en las esferas técnicas y tecnológicas de la ingeniería de sistemas informáticos. Así, este conjunto de técnicas y herramientas procuran ser aplicables tanto en las etapas pre-informáticas (en las que la información es manejada y recopilada de manera manual) como en las fases de tratamiento automatizado posibilitadas por la informática (definida por Riascos Gómez como *"la ciencia del tratamiento lógico, sistematizado e informatizado de cualquier unidad de información o datos"* (Riascos Gómez, 1999, pág. 125), por lo que se puede asegurar que nos hallamos ante un campo que requiere, por su naturaleza misma, de la cooperación interdisciplinaria.

Desde el punto de vista legal, la protección de datos personales ha sido definida como *"la protección jurídica de las personas en lo que concierne al tratamiento de sus datos de carácter personal, o de otra forma, el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para confeccionar una información que, identificable con él, afecta su entorno personal, social o profesional, en los límites de su intimidad, incide directamente en un derecho fundamental de elevado contenido"* (Conde Ortiz, 2005).

### *Problemática del Tratamiento de los Datos Personales*

La protección de datos personales se encuentra fundamentada en la necesidad de encontrar maneras de salvaguardar la dignidad humana y brindar un necesario equilibrio entre los derechos fundamentales de intimidad, privacidad e información en un contexto histórico y social que requiere, con cada vez mayor intensidad, la permanente cesión de los datos del individuo a infinidad de sistemas de información por los más diversos fines.

La problemática que actualmente confronta a la protección de datos fue elocuentemente plasmada por Rodríguez Pérez, quien afirma que gracias a las bases de datos, en la actualidad *"se dispone de un conjunto de datos que, convenientemente tratados de forma automática, en relación con un fin determinado, proporcionan información sobre la persona.*

*La inteligencia artificial ofrece hoy la posibilidad de comparar, interrelacionar y analizar los datos de una persona, proporcionando un perfil de la misma. Pero, además cabe que la comparación se establezca respecto de un modelo o perfil predeterminado, advirtiendo de los datos de la persona que se desvían del modelo y poniendo a disposición del responsable del fichero información sobre las conclusiones que se derivan de esa desviación. Si a todo esto se añade la ayuda que proporcionan las comunicaciones y la transferencia de datos telemáticos, puesto que permiten el cruce de ficheros y registros informáticos, así como el correspondiente tratamiento de los mismos, nos encontramos con que la persona pierde el control sobre la utilización que se pueda hacer de sus datos personales y que la información parcial*

*proporcionada en un principio, de por sí valiosa, se convierte en valiosísima, con lo que ello significa en el aumento de la cota de poder del responsable del fichero, esto es, la persona física o jurídica, pública o privada, que decide sobre la finalidad, contenido y uso del fichero y su tratamiento"* (Rodríguez Pérez, 2003, pág. 3).

El panorama actual que presenta la sociedad de la información y la comunicación, tiene como consecuencia fundamental la vulnerabilidad del individuo frente al tratamiento automatizado de sus datos personales por parte de terceros que pueden incluso serle desconocidos.

De acuerdo con Milán Salas & Peralta Ortega, el continuo desarrollo de las tecnologías de la información y la comunicación ha dado a lugar al surgimiento de interrogantes y preocupaciones desde los siguientes puntos de vista:

*"Tecnológico: hay que velar por la seguridad de las redes de telecomunicaciones, e impedir las accesos (sic) no autorizados a los centros de proceso de datos.*

*Económico: los datos no son ya simplemente informaciones que se solicitan para prestar servicios o bienes por la Administración o las empresas, sino que se les considera elementos susceptibles de tráfico económico, mercancías, se les asigna un valor económico y se fomenta su intercambio. Surge una tensión entre el libre flujo de información, que hay que proteger, en una sociedad cada vez más interconectada, y la protección de la persona y la garantía de sus derechos y libertades.*

*Político: hay que conjugar el derecho de acceso a las Bases de Datos de la Administración Pública con la seguridad del Estado y la defensa nacional. (Son célebres el debate suizo sobre el secreto bancario o la polémica italiana sobre el secreto de Estado).*

*Sobre todo, desde el punto de vista de los ciudadanos, que ven perdido el control de sus datos personales, con la inquietud de que éstos puedan ser utilizados, no para prestarles un servicio, que es para lo que se cedieron, sino para lesionar sus bienes o derechos. Éste es el especial problema jurídico que se plantea: cómo regular el control del tratamiento automatizado de los datos de carácter personal" (Millán Salas & Peralta Ortega, 1995, págs. 2-3).*

Esta problemática ha sido también aludida por Chirino, quien recuerda que: *"Estamos viviendo en la actualidad un verdadero movimiento en el llamado "ambiente de la información", donde los datos e informaciones han adquirido un enorme valor económico"* (Chirino, 1997, pág. 1), en el cual, solo queda admitir la innegable transparencia de nuestra personalidad virtual ante los sistemas de información y comunicación.

En el contexto resultante de este conjunto de inquietudes, y especialmente ante la actual tendencia hacia la monetización de los datos personales, vuelven a adquirir relevancia aquellas dos premisas fundamentales señaladas por Warren & Brandeis en sus ensayos sobre el derecho a la privacidad, que rezan: a) que todo individuo debe gozar de total protección en su persona y en sus bienes *(Riascos Gómez, 1999, pág. 37)* (entendiéndose extendida tal protección a los bienes morales del individuo); y b) la consideración del principio de inviolabilidad de la persona (y de la propia personalidad) como extensible incluso a la protección de los pensamientos, sentimientos y emociones del individuo ante su comunicación por parte de terceros sin importar el medio *(Riascos Gómez, 1999, pág. 40 y 42)*.

En los esfuerzos por la búsqueda de soluciones holísticas y equilibradas ante la aparente dicotomía existente en la actualidad entre el tratamiento de la información y los derechos fundamentales, recordar las premisas de Warren & Brandeis permitirá

comprender que aún en un contexto en el que el derecho a la privacidad sea observado desde una concepción puramente patrimonial y disponible, no deben ser olvidados nunca los derechos humanos del individuo que permiten el libre ejercicio de la autodeterminación humana en un marco de inviolabilidad personal y patrimonial.

Asimismo, se debe recordar que la autodeterminación informativa mantiene su carácter de derecho humano, *"inherente a la persona e indisponible. Sin embargo, la autodeterminación conlleva, además de facultades meramente ejercitables, la posibilidad de ceder un dato concreto y determinado. Ello no equivale a una patrimonialización del derecho, pero sí del dato que puede convertirse en objeto negocial, gratuito u oneroso (imaginemos que se revelan más datos de los necesarios a cambio de una rebaja en el precio), del mismo modo que una persona puede vender una parcela de intimidad. De hecho las empresas de publicidad comercian con ellos de forma más o menos elaborada. Esta cesión debe ser individual, concreta y contemporánea o al menos determinable, de forma que no llegue a comprometer la subsistencia del propio derecho"* (Barral Viñals I. , 2003, pág. 2), por lo que, de contar con un marco técnico y legal que asegure suficiente protección al individuo, la monetización de los datos personales no implica necesariamente una afectación a nuestra dignidad o a nuestros intereses.

### *Objetivos de la Protección de Datos Personales*

En tanto la protección de datos personales procura la manifestación del derecho a la autodeterminación informativa en el contexto actual, puede asegurarse que subsume dentro de sus objetivos tanto la protección del bien jurídico tutelado por este derecho

(la libertad individual); como la protección de todos aquellos datos que configuran y rodean la información personal (datos y metadatos), los cuales adquieren valor por medio de su interconexión y contextualización[58].

La protección de datos tiene como objetivo fundamental el tornar eficaz el derecho de autodeterminación informativa, procurando mediante su visión iusinformática la protección de los datos y metadatos referidos a personas identificadas o identificables *"Contra cualquiera que realice actividades de acceso, registro, tratamiento y transferencia de datos y que esos datos trasciendan a terceros"* (Solorio Pérez, 2009, pág. 5).

Los datos personales, en el contexto de la protección de datos, son protegidos frente a aquellas situaciones capaces de afectar negativamente los intereses de sus respectivos sujetos de datos. Dentro de estas situaciones, pueden encontrarse las siguientes: (Solorio Pérez, 2009, pág. 5):

- Tratamiento sin consentimiento
- Acceso por terceros no autorizados

[58] De esta manera puede considerarse que la protección de datos personales no solamente debe verse limitada a aquellas informaciones directamente relacionadas con la persona y/o recopiladas directamente de su parte, sino también a aquellos datos que sean generados a partir de dicha información.
Un ejemplo práctico de esta situación puede ser encontrado en la información generada por los sistemas de identificación biométrica por parte de la red social Facebook, los cuales a la fecha son considerados tan exactos como el cerebro humano (Yang, Ming; Ranzato, Marc' Aurelio; Wolf, Lior, 2014). A lo largo del proceso de procesamiento de la información facial, estos sistemas utilizan tanto información personal (la imagen del individuo, obtenida "voluntariamente" por quien sube su fotografía a la red social) como información generada a partir de las fotografías (por ejemplo, identificadores faciales predefinidos o puntos de referencia generados por el sistema mismo) la cual no es liberada a los usuarios puesto que esta información es propiedad de la empresa (la empresa únicamente libera el número de identificación de su archivo, pero no les permite acceder a una copia de la información cruda generada por el sistema "Deep Face") (Epic.org, 2011).
Una aplicación real de los derechos comprendidos bajo la Protección de Datos Personales (y específicamente del derecho humano a la autodeterminación informativa) debería de reconocer la necesaria relación existente entre este conjunto de metadatos agregados con el individuo afectado, a la vez que le permita ejercer el control sobre la totalidad de la cadena de tratamientos realizados a sus datos personales (sobre las posibilidades reales de los metadatos ver: (Cavoukian, 2013)).

- Registro de datos no autorizados
- Datos incorrectos
- Registro por tiempo indefinido
- Tratamiento ilegítimo
- Utilización abusiva
- Obtención por medios fraudulentos
- Transferencias internacionales de datos no autorizadas

Frente a este conjunto de objetivos, se torna especialmente relevante la opinión de González Murúa, quien demarca también la diferencia entre la protección de datos personales y la mera protección de los ámbitos de intimidad, al afirmar que:

*"La técnica de la protección de datos no se centra ni mucho menos con exclusividad en lo que se viene entendiendo como intimidad. En opinión de Lucas Murillo de la Cueva "si éste fuese el bien jurídico por defender, lo que habría que resguardar del peligro informático sería bastante poco". Sin embargo ciertos datos que en principio parecen inocuos, o que no guardan ninguna relación con la intimidad como el supuesto de tener o no un automóvil o de ser cliente de una entidad financiera determinada, u otras informaciones como la raza, la adicción religiosa o la filiación política o la conducta sexual incluso cuando se explícita públicamente en determinados colectivos como forma de protesta, -y , especialmente estos últimos a pesar de que hubieran perdido la condición de íntimos por hacerlos públicos la persona son los que necesitan una tutela legal eficaz frente a su tratamiento automatizado, cesión, etc." (González Murúa, 1994, pág. 14).*

De esta manera podrá comprenderse ahora que la protección de datos personales no puede verse reducida únicamente a la protección de aquellos que se encuentren en un

contexto dado, sino que deberá abarcar todos los datos y metadatos que se encuentren en una situación de susceptibilidad "*de tratamiento o se encuentren en soporte susceptible de tratamiento, b) Que se tenga la posibilidad de identificar el resultado del tratamiento de los datos con su titular y c) Que el manejo o acceso a los datos resulte sin consentimiento de su titular"* (Conde Ortiz, 2005).

Asimismo, debe recordarse que la protección de datos procura llevar a cabo sus objetivos por medio del establecimiento y aplicación de fuentes (tanto normativas como técnicas y contractuales) tales como la Constitución Política de cada país, la legislación general y sectorial aplicable, contratos, acuerdos, códigos de conducta, estándares técnicos, modelos de "buenas prácticas", convenios y tratados internacionales.

Finalmente, en tanto la protección de datos personales busca fundamentalmente brindar efectividad al derecho de autodeterminación informativa, esta debe tomar en consideración límites similares a los que tal derecho posee, a saber: *"la seguridad del Estado; la seguridad Pública, la prevención e investigación de infracciones penales; el interés económico del Estado y los derechos y libertades de otros individuos"* (Solorio Pérez, 2009, pág. 5).

## *Sujetos de la Protección de Datos Personales*

### *Sujeto Activo*

A partir del estudio realizado hasta el momento, no debe resultar sorprendente para el lector que se afirme, sin mayor miramiento, que toda persona posee titularidad activa en la protección de sus datos personales. Efectivamente, a partir de sus fundamentos en el derecho a la autodeterminación informativa y la dignidad humana, la identidad del sujeto activo de tal protección pareciera evidente.

A pesar de tal apariencia, una mirada más detallada a la afirmación anterior despierta una duda principal: al afirmar que **toda persona** es sujeto activo de la protección de sus datos personales, ¿se hace referencia tanto a las personas físicas como a las jurídicas?

No es posible encontrar una simple solución a esta interrogante, dado que usualmente la determinación de la titularidad sobre tal protección es establecida en el nivel estatal (lo cual genera un panorama sumamente variable). Pese a tal situación, se puede comenzar a solventar este problema afirmando lo evidente: en tanto se encuentran fundamentadas en derechos humanos, las técnicas y herramientas correspondientes a la protección de datos personales indudablemente legitiman a toda persona física para que adopte el rol de sujeto activo.

Ahora bien, resulta comprensible la existencia de posiciones encontradas a la hora de extender a las personas jurídicas la titularidad sobre un derecho que históricamente ha sido asociado con el honor, la privacidad y la intimidad[59]; especialmente dada la confusión entre protección de datos, habeas data y autodeterminación informativa anteriormente mencionada.

[59] Los cuales han sido usualmente considerados inherentemente "humanos" y que a lo largo de la historia no han sido extendidos a las personas jurídicas dado que a ellas son normalmente aplicados recursos como el secreto corporativo y el velo societario como medios para defender su información.

Tal asociación deja de ser aplicable en el caso del derecho a la autodeterminación informativa en tanto, - tal como se explicara con anterioridad - este derecho se extiende más allá del ámbito de tutela de la privacidad y la intimidad para proteger un bien jurídico tutelado de gran relevancia, tanto para personas físicas como jurídicas.

La titularidad de las personas jurídicas en la protección de sus datos personales ha sido objeto de debates acalorados entre los doctos en la materia, a lo largo de los años. Así, algunos de los argumentos que esgrimidos en oposición al reconocimiento de las personas jurídicas pueden ser identificados, han sido los siguientes:

1) *"Los bienes, derechos o intereses que se tutelan en el caso de las personas físicas y en el de las jurídicas son diferentes.*
2) *En el debate doctrinal de los países que consideran extender el campo de aplicación de la protección de datos a las personas jurídicas se piensa fundamentalmente en las empresas y asimismo se habla sobre lo innecesario de extender un derecho humano cuando las empresas cuentan con la protección de otras ramas del derecho, llegándose incluso a afirmar que "mientras en las personas físicas lo que se protege es la "l", en las personas jurídicas lo que se protege es la "sunshine", es decir, la publicidad. En el caso de las empresas no resulta, siempre y en todo caso, interesante la transparencia. El derecho de acceso podría ser enormemente negativo para la libre competencia"* (González Murúa, 1994, pág. 19).

En contraposición con los argumentos anteriormente mencionados, González Murúa identifica algunos de los argumentos que han sido utilizados para defender la titularidad de las personas jurídicas sobre la protección de sus datos, a saber:

1) *"La admisión de la titularidad de las personas jurídicas sobre el derecho a la aplicación de la protección de datos se veía usualmente frustrada por la consideración legal de la protección de datos como mera manifestación de la protección de la intimidad, la vida privada y las libertades individuales encontradas solamente en las personas físicas. Sin embargo, el considerar la protección de datos como manifestación del derecho de autodeterminación informativa posibilita extender el ámbito de aplicación de las leyes de protección de datos incluso a personas jurídicas.*
2) *Tanto personas jurídicas como físicas pueden tener interés en ejercitar el derecho de acceso, de rectificación o de cancelación de datos inexactos, falsos, desfazados, etc. como parte de su derecho de autodeterminación informativa con miras a evitar los perjuicios relacionados con la divulgación de dichos datos.*
3) *El derecho de autodeterminación informativa funciona como un derecho-garantía de todos los derechos de las personas. Evidentemente, tan amplia afirmación incluye, como señalamos anteriormente, derechos como el honor o la intimidad que solamente son atribuibles a personas físicas, pero también incluye "derechos no fundamentales o intereses" de los que pueden ser titulares tanto personas físicas como jurídicas, para los que el cumplimiento de los principios de Principios de Calidad de los Datos anteriormente estudiados pueden evitar perjuicios a sus intereses (como la denegación de un crédito)"* (González Murúa, 1994, pág. 20).

El debate sobre la titularidad de las personas jurídicas en la protección de sus datos personales se encuentra aún vigente. En algunas jurisdicciones, como por ejemplo en España, se afirma que la protección de datos no resulta aplicable a los datos referidos a personas jurídicas (si bien se permiten ciertas actuaciones por parte de estas en materia penal, con miras a su protección frente a ilícitos como el robo de datos por

medios informáticos, entre otros); mientras que en otras jurisdicciones se considera que la protección de datos personales aplica a personas físicas y jurídicas por igual.

Tal como se estudiara en los capítulos finales de la presente investigación, el sistema actualmente vigente en Costa Rica se asemeja en este sentido a la jurisdicción española. En nuestro país la materia se encuentra regulada tanto por la Ley Nº 8968 de Protección de la Persona frente al tratamiento de sus datos personales, como por las disposiciones de la Ley Nº 9048 sobre Delitos Informáticos (entre otras). Paradójicamente al realizar un estudio de ambas normativas se tiene, que mientras que la Ley Nº 8968 rechaza absolutamente a las personas jurídicas como sujetos activos de la protección de datos personales, las disposiciones de la Ley Nº 9048 admiten expresamente tal posibilidad[60].

De conformidad con lo anterior, es posible aseverar que en Costa Rica no es extendida a las personas jurídicas el derecho de autodeterminación informativa, a pesar de lo cual se les reconoce la potestad de incoar procesos por violación a los datos personales de terceros que se encuentren en sus bases de datos (o incluso aquellos datos correspondientes únicamente a la persona jurídica[61]).

Debe considerarse que este sistema es válido en tanto la protección de datos personales procura hacer efectivo el derecho de autodeterminación informativa, el cual, tal como se estudiara ya en el primer capítulo, es atribuible a todo ser humano

[60] Así, si bien es cierto que nuestra legislación no reconoce a las personas jurídicas como sujeto activo del derecho de autodeterminación informativa en sedes civil y administrativa, en sede penal es posible encontrar una excepción en el artículo 196 bis mediante la cual se sanciona la violación de datos de personas físicas o jurídicas.

[61] Por ejemplo, podría incoar una persona jurídica un proceso por violación de datos personales en sede penal siempre que datos de terceros bajo su tutela o datos propiamente suyos (tales como la balanza económica, el registro de sus accionistas, u otros tipos de información privada o reservada a sus socios) almacenados en medios informáticos sean violentados u afectados.

por el mero hecho de serlo. En tanto el bien jurídico tutelado por la autodeterminación informativa no es otro que la libertad humana[62], la posibilidad de reconocer a una persona jurídica como sujeto activo de la protección de datos personales resulta inconveniente en tanto estas no son por sí mismas seres humanos[63].

Ahora bien, esta negación a la capacidad de las personas jurídicas de incoar procesos administrativos de protección de datos personales invocando su derecho a la autodeterminación informativa no se traduce en nuestro país en una situación de indefensión para estas. Las personerías jurídicas se rigen en Costa Rica por un marco jurídico determinado que prevé mecanismos como el *secreto corporativo* y los métodos de protección de la propiedad intelectual con miras a garantizar la seguridad de la información propiedad de las empresas; pero más allá de esta protección, debe recordarse que estas cuentan con el deber y el derecho de implementar las técnicas de seguridad de la información en sus sistemas informáticos y, tal como establece la Ley Nº 9048, pueden incoar siempre procesos penales con tal de castigar la vulneración y el tratamiento no autorizado de sus datos personales.

En otras palabras, si bien el sistema jurídico vigente en nuestro país reserva únicamente a las personas físicas la titularidad sobre el derecho a la

[62] Debe recordarse también que el derecho a la autodeterminación informativa, puesto en acción mediante las técnicas iusiformáticas de la protección de datos personales procura defender al individuo de las limitaciones a su derecho a la libertad. Toda persona debe ser capaz de vivir su vida libre de la constante amenaza de ver todas sus acciones examinadas, contrastadas y (des)contextualizadas por un gran hermano omnisciente.
Frente a este derecho, las nuevas tecnologías facultan a quien posea las capacidades tecnológicas de llevar a cabo dicho control sobre los individuos, planteando con ello un serio obstáculo a la autodeterminación humana, la cual ahora se encuentra constantemente coartada por la autocensura ante la amenaza de que sus datos, gustos y pensamientos más íntimos sean publicados o utilizados en su contra.

[63] Más aún, debe recordarse también que cada vez es más común que estas mismas personas jurídicas (y ya no solamente los Estados) sean responsables de la violación de los datos personales.

autodeterminación informativa, esta reserva no se ve directamente traducida en las disposiciones sobre protección de datos personales. Mientras que nuestra Ley de protección de la persona frente al tratamiento automatizado de sus datos personales protege únicamente a la persona física por medio de los procesos administrativos ante PRODHAB, nuestra ley de delitos informáticos legitima también a las personas jurídicas para proteger sus datos personales en sede penal.

En opinión del suscrito autor de esta investigación, esta protección bipolar se basa en la necesidad de brindar mayor protección al ser humano, para lo cual la legislación costarricense contempla dos bienes jurídicos tutelados por la protección de datos personales: por un lado la vía administrativa busca la protección de la libertad humana (bien jurídico tutelado del derecho humano a la autodeterminación informativa), mientras que por otro lado, nuestra legislación penal protege a la información y al dato (personal o no) como bien jurídico tutelado ante los delitos informáticos[64].

*Sujeto Pasivo*

Todo administrador o encargado de dar tratamiento a una base de datos se constituye como sujeto pasivo de la protección de datos personales independientemente de si pertenece al sector público o privado. Así, tanto los gobiernos y sus poderes públicos como los sujetos de derecho privado se encontrarán bajo las disposiciones legales y

[64] En este punto es recomendable revisar la legislación colombiana examinada a lo largo del capítulo de derecho comparado de la presente investigación, pues en nuestra opinión nuestra ley Nº 9048 presenta múltiples paralelismos con la ley 1273 de 2009.

técnicas relevantes que sean aplicables para la protección de los datos y metadatos de carácter personal que tales entes tengan a su disposición.

Al igual que en el caso de los sujetos activos, al determinar a los sujetos pasivos de la protección de datos personales se está frente a un problema fundamental: el carácter territorial de la normativa estatal utilizada hasta el momento en la regulación de la materia, conlleva severas dificultades a la hora de aplicar la ley a los administradores de bases de datos ubicadas fuera del territorio nacional.

Asimismo, debe resaltarse que con el surgimiento de la *web 2.0*[65] (y ni qué decir sobre la futura *web 3.0*[66]), los modelos tradicionales de administrador/sujeto de datos han comenzado a cambiar. En la actualidad se dan situaciones en las cuales los individuos son considerados como verdaderos pares, que comparten y reciben información en igualdad de condiciones, por lo que se constituyen ellos también en administradores de datos; esto ha traído nuevos retos al mundo de la protección de datos personales, siendo necesarios nuevos esfuerzos por educar a todos los interesados en una cultura respetuosa de los datos personales.

El problema de las transmisiones transfronterizas de datos personales y el carácter extraterritorial de estos será tratado de manera más extensa a lo largo de la presente

[65] Término utilizado a partir del año 1999 para describir aquellos sitios web que no se encuentran limitados a brindar al usuario texto estático, sino que le permite interactuar con las páginas y colaborar con otros usuarios en tiempo real mediante nuevas herramientas tales como los medios sociales, las comunidades virtuales, etc. Se trata de una red marcada por el diálogo de los usuarios que se constituyen en creadores y consumidores activos de contenidos multimedia.

[66] Término utilizado para hacer referencia a las futuras versiones del Internet cuyas características específicas aún no podemos imaginar pero que probablemente se encuentre dirigido hacia la personalización de la red, la creación de la llamada “web semántica” (una red en la que las computadoras son capaces de entender peticiones humanas complejas a partir de su significado) y su integración con tecnologías que permitan la convergencia entre el mundo real y el Internet (Metaverso), tales como la realidad aumentada y el Internet de las cosas.

investigación; así, bastará por el momento señalar que idealmente, todo mecanismo legal o técnico que pretenda asegurar la protección de los datos personales en el mundo moderno deberá considerar como un objetivo fundamental el permitir a todo sujeto de datos ejercer eficazmente su derecho a la autodeterminación informativa frente a cualquier administrador de bases de datos o procesador de datos personales, con independencia del carácter público o privado de este y de la naturaleza, fin o ubicación geográfica de la base de datos.

### *Objeto de la Protección de Datos Personales*

Como su nombre lo indica, la protección de datos personales se preocupa por la protección de la información de un individuo. Ante una definición tan simple, necesariamente surgirá en el lector una gran cantidad de interrogantes, dentro de las cuales se pueden considerar como fundamentales dos preguntas: ¿Qué debe entenderse por información? Y ¿qué datos constituyen información personal?

La respuesta a la primera interrogante solamente puede ser respondida acudiendo al punto de vista holístico e interdisciplinario propio del Derecho Informático.

El término *"información"* es definido según la informática como *"un proceso físico-mecánico de transmisión de datos como elemento referencial acerca de un hecho. En sentido general, un conjunto de datos constituye una información"* (Téllez Valdés, 2003, pág. 58). Asimismo, para esta ciencia, un dato es aquella información capaz de ser procesada por un sistema (automático o manual).

En contraposición, el punto de vista legal examina el concepto de información brindándole una connotación *"vinculada a la libertad, refiriéndola a la opinión y expresión de ideas por cualquier medio que sea"* (Quiroz Ruiz, 2004, pág. 4), en la que los *"hechos nacientes en la [sic] una perspectiva histórica, económica, política, cultural, científica, o técnica de la sociedad, constituyen los datos en cada uno de esos ámbitos"* (Quiroz Ruiz, 2004, pág. 4).

En tanto el Derecho basa su examen de la información desde el punto de vista lingüístico y contextual, se puede definir el concepto de "*datos"* según los lineamientos del diccionario de la Real Academia Española como el *"Antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho"* (Real Academia Española, 2001).

El examen, desde la perspectiva iusinformática, de las definiciones anteriores, permitirá afirmar que puede entenderse por información a *todo conjunto de datos que procure la comunicación de cualquier hecho por cualquier medio, siempre y cuando tal comunicación sea capaz de ser analizada y procesada sistemáticamente.*

Tal como se observó con anterioridad, el verdadero valor de los datos se encuentra en su capacidad de ser contextualizados. Tanto la definición de dato brindada por la perspectiva informática como la que provee el diccionario de la Real Academia transmiten la idea de que los datos aislados y circunscriptos poseen por sí solos muy poco valor (Bolaños Chaves, 2012, págs. 20-22), pero en el momento en que estos son contextualizados (mediante su agregación con otros datos y metadatos), se convierten en información y su valor crece de manera exponencial.

Con base tan solo en el valor contextual de la información, se puede dar inicio a la solución de la segunda pregunta planteada, afirmando que el objeto ideal que buscan proteger las técnicas y herramientas de protección de datos personales debe ser *toda información (así como toda información sobre la información) relacionada con una persona identificada o identificable.*

Desde esta perspectiva ideal (basada en los postulados fundamentales del derecho de autodeterminación informativa), se puede afirmar que ningún sistema de protección de datos que pretenda cumplir a cabalidad su papel en la actualidad, debe permitir que el objeto de la protección se limite solamente a datos específicos o a ciertos tipos de datos, dado que la afectación potencial a la que se expone el individuo crece exponencialmente ante el manejo de cualquier información que le identifique.[67]

Así, la protección de datos personales no debe considerar ajenos aquellos datos que en la actualidad son vistos como externos al ámbito sensible del individuo; debe procurar proteger todo dato que pueda conducir a la creación de perfiles individuales aun cuando estos en la actualidad sean considerados inútiles por relacionarse con nuevas tecnologías aún no aplicadas a gran escala.

La protección ideal de los datos personales debe aceptar como necesaria la protección holística de la información individual, incluyéndose dentro de los datos personales todos aquellos cuya recopilación, tratamiento o difusión pueda afectar los intereses de su titular.

[67] Y tal como se estudiará en la segunda sección del presente capítulo, en la actualidad toda información puede identificar a su titular al ser procesada, agregada y recontextualizada aún tras haber sido liberada de manera anónima (Ohm, 2009).

*Breve Tipología de los Datos Personales*

Tal como se afirmó con anterioridad, una clasificación general de la información afirma la existencia de información pública, información de interés general e información privada. En tanto esta información se encuentra compuesta por datos de diversos tipos, es posible identificar ciertos datos como públicos (estado civil, posesión de bienes muebles o inmuebles, u otros) o privados (orientación sexual, etnia, credo religioso, entre otros), los cuales podrán ser sujetos de tratamiento cuando medien razones de interés general autorizadas por ley.

Dentro de los datos privados pueden encontrare los datos personales, los cuales son comprendidos por el *World Economic Forum*[68], como aquellos *"datos o metadatos (datos sobre los datos) relacionados con una persona específica, identificada o identificable"* (World Economic Forum, 2012, pág. 7).

Antes de desarrollar con mayor profundidad el estudio de la protección de datos, resultará adecuado presentar al lector una breve introducción a las diversas clasificaciones en las cuales pueden ser divididos los datos personales. Para ello se seguirá la lista creada por Davis, Martínez & Kalaboukis, a partir de la cual Hamlin (Hamlin, 2011) crea su mapa de los tipos de datos personales (Anexo 4).

[68] En la actualidad no existe una definición inequívoca sobre el concepto de datos personales dado que este concepto ha sido abordado desde diversas perspectivas por los entes legislativos del mundo. A pesar de lo cual, la definición provista se adecúa en términos generales con lo establecido tanto por la Privacy Bill of Rights estadounidense como por la legislación europea vigente sobre protección de datos

- Datos Contextuales: Son todos aquellos datos que tienen que ver con el contexto general de la persona, lo cual incluye a las personas y objetos que le rodean, los eventos importantes de su vida (incluyéndose con ellos los datos de su calendario y los datos de eventos brindados por servicios web) y los datos de localización[69] (pasados, actuales y futuros) de la persona.
- Datos de Contenido: Aquellos datos e informaciones encontradas dentro de los documentos privados del individuo y en los medios que el individuo consume a lo largo de su vida (libros, fotografías, videos, música, podcasts, software, otros).
- Datos de Registros Gubernamentales: Dentro de los que se pueden encontrar aquellos datos encontrados en registros públicos, tales como el o los nombres del individuo, los eventos de los cuales existe certeza pública concernientes al individuo (registro de nacimiento, matrimonios inscritos, divorcios y certificación de defunción), los registros de procesos legales en los que se haya visto involucrado el individuo, su historial criminal, otros.
- Datos Financieros: Relacionados con el estado financiero del individuo y que incluyen tanto los datos relacionados con los bienes virtuales que posee este, como los registros existentes sobre bienes físicos poseídos.. Asimismo, los datos financieros incluyen la información sobre los activos que percibe el individuo, sus pasivos, las transacciones que realiza, sus

[69] Definidos por Barral Viñals como aquellos datos " tratados en una red de comunicaciones electrónicas que indican la posición geográfica del equipo terminal del usuario (art. 2.c Directiva 2002/58/CE). Los servicios de redes celulares u obtenidos por satélite manejan datos como la latitud, longitud y altitud del terminal, la dirección de la marcha, el nivel de precisión de la información de localización o la hora de registro de la información. Son datos que, por ejemplo, permiten disfrutar de servicios de emergencia o de valor añadido, pero que también se prestan a usos invasivos para la persona. " (Barral Viñals I. , 2003, pág. 6).

cuentas, sus obligaciones, los datos relativos a los seguros que posea, su participación en asociaciones, sus impuestos y su calificación crediticia.

- Datos Médicos: Aquellos datos relacionados con el historial médico del individuo (su información genética, los tratamientos a los que ha sido sometido, entre otros) y los datos relacionados con su seguro médico.
- Datos de Actividad: Son los datos relacionados con toda actividad realizada por el individuo tanto en el mundo real (preferencias alimenticias, horario de sueño, compras realizadas, historial de manejo de vehículos, entre otros) como en el ciberespacio (aplicaciones utilizadas, sistema operativo preferido, explorador web utilizado y otros).
- Datos del Portafolio Electrónico: Los cuales hacen referencia al historial laboral o académico del individuo, incluyendo sus creaciones y cartera de clientes.
- Datos de Identidad: Dentro de los que están los identificadores de identidad utilizados por el individuo en sus relaciones virtuales y físicas (nombres de usuario, direcciones de correo electrónico, números telefónicos, apodos, avatares, otros); sus intereses (“likes”, elementos favoritos, etiquetas, preferencias y configuraciones utilizadas en los diversos programas utilizados); los elementos identificadores de los dispositivos electrónicos utilizados por el individuo (dirección IP asignada por su operador de telecomunicaciones, dirección MAC del dispositivo, identidad del dispositivo “bluetooth”, nombre de la red de internet inalámbrica de su hogar, tarjeta SIM asignada a su cuenta celular, Número IMEI de su celular,

entre otros); y sus datos demográficos (edad, sexo, dirección, nivel educativo, experiencia laboral, curriculum vitae, entre otros).

- Datos Derivados del Consumo de Contenidos: Definidos por Barral Viñals como *"aquellos que circulan por la Red. Los proveedores de servicios pueden tratar datos reveladores de la identidad, dirección, gustos y aficiones, poder adquisitivo u otras características personales de los usuarios. Piénsese en los datos de registro (en foros de debate, suscripciones o tiendas virtuales), los hábitos de compra o el volumen de gasto y forma habitual de pago, que se vinculan a una persona a través de cookies o, simplemente, con los datos precisos para la entrega domiciliaria (el comercio electrónico ha supuesto un impulso para la logística o distribución, sin perjuicio de los productos que se adquieren directamente a través de la red* (Barral Viñals I. , 2003, pág. 6).
- Datos Relacionales: Los cuales incluyen elementos como sus contactos de la libreta de direcciones (física y digital) del individuo, sus amigos y círculos de conocidos en redes sociales, su información familiar y genealógica, su membrecía a grupos determinados y su historial de llamadas y mensajes.
- Datos de Comunicación: Son todos los datos relacionados con las comunicaciones establecidas por el individuo por cualquier medio, desde las conversaciones orales por cualquier medio; hasta sus comunicaciones escritas (carta, mensajería instantánea, SMS, correo electrónico, hipervínculos compartidos y actualizaciones de estado) y su participación en medios sociales (fotografías, videos, videoconferencias, "hangouts", apariciones televisivas y musicales, entre otros).

- Datos de Transmisión: Los cuales se encuentran conformados por el conjunto de registros y transacciones realizadas a lo largo del uso común de las tecnologías de la información y la comunicación que conforman también la llamada "digital footprint" del individuo en su paso por el Internet. Según Barral Viñals, *"Los datos de la transmisión comprenden los datos del tráfico y de localización. Es un dato sobre el tráfico cualquier dato personal tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de facturación de la misma. Incluyen las conversiones efectuadas a través de la red a efectos de realizar la transmisión. Los operadores de infraestructuras o redes de comunicaciones, comprendidas las inalámbricas, o los servidores de acceso registran datos como el encaminamiento, la duración, hora o volumen de la comunicación, datos relativos al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión o al formato de la transmisión. Los proveedores de servicios que almacenan páginas web y prestan servicios como correo electrónico o foros de debate registran las páginas web visitadas y pueden establecer el llamado rastro de clicks. Debe tenerse en cuenta que la cabecera HTTP proporciona datos como el sistema operativo, tipo y versión del navegador, idioma utilizado o página de proveniencia"* (Barral Viñals I. , 2003, pág. 5).

Finalmente, debe recordarse también que en Costa Rica la Ley Nº 8968 de Protección de la persona frente al tratamiento de sus datos personales clasifica los datos personales dentro de tres sub-clasificaciones fundamentales, a saber:

- Datos Sensibles: aquella *"Información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros"* (Asamblea Legislativa de la República de Costa Rica, 2011).
- Datos Personales de Acceso Restringido: Son *"los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública."* (Asamblea Legislativa de la República de Costa Rica, 2011)
- Datos Personales de Acceso Irrestricto: Son *"los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados"* (Asamblea Legislativa de la República de Costa Rica, 2011).

### *Principios Legales Generalmente Aplicables al Objeto de la Protección de Datos*

Una vez comprendida la verdadera extensión de aquellos datos considerados personales, debe realizarse un breve análisis de los principios que rigen de manera general su protección en nuestra realidad.

Fundamentalmente, debe comprenderse que a la fecha no existe un sistema capaz de llevar a la realidad la protección holística que busca la protección de datos personales. Los sistemas actuales de protección de datos se enfrentan constantemente a la dicotomía existente entre la necesidad de proteger los derechos de privacidad y de

autodeterminación informativa de los usuarios de las redes de telecomunicaciones y el necesario fomento de las actividades productivas en un mundo interconectado.

Tal como se mencionara anteriormente, ante esta realidad, el derecho de autodeterminación informativa procura alivianar la dificultad de la protección de los datos del individuo, mediante la admisión de su capacidad para liberar sus datos como considere conveniente, así como ciertos límites a la protección debida al titular de dichos datos.

Esta función del derecho a la autodeterminación informativa se encuentra fundamentada en una serie de principios generales que, según Riascos Gómez, *"no son meras declaraciones pragmáticas establecidas por el legislador, sino contenidos axiológicos que sirven a unos fines u objetivos de la materia objeto de la misma ley y que por esto son de la esencia en la interpretación o hermenéutica jurídica de los asuntos relacionados. En otros términos, son contenidos de esencia, presencia y decisión de un continente o materia específica"* (Riascos Gómez, 1999, pág. 108 vol. 2).

En la protección de datos personales entonces, debe recordarse la existencia de tres principios generales aplicables a los datos y que trabajarán en conjunción con varios principios específicos que serán aplicables a las diversas etapas del tratamiento de los datos. Estos tres principios generales son:

- Principio de Libre Circulación de la Información

  Principio general de las redes de telecomunicaciones modernas, recuerda los modelos descentralizados utilizados en la actualidad en los cuales se pretende evitar a toda costa las restricciones a los flujos globales de información y las

afectaciones innecesarias a la innovación y el intercambio facilitados por las tecnologías de la información y la comunicación.

Se relaciona con la materia del presente estudio, en tanto protege el derecho de autodeterminación informativa, el derecho a la información y el derecho a la libre expresión con la ayuda del principio de restricción legítima.

Mediante el aseguramiento de la libre circulación de los datos por las redes globales, este principio procura fortalecer las redes de telecomunicaciones evitando la creación de barreras que generen tratos discriminatorios en el nivel nacional e internacional, por lo que se relaciona también con los principios rectores establecidos en la Ley General de Telecomunicaciones No. 8642, especialmente con los de universalidad, no discriminación y neutralidad tecnológica.

Se trata de un principio reconocido con anterioridad en diversos marcos normativos, siendo de especial importancia en el ámbito internacional las disposiciones del Convenio 108 del Concejo de Europa, el cual establece en su artículo 12, inciso 1 que por regla general, *"una parte no podrá, con el único fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra parte"* (Consejo de Europa, 1981).

- Principio de Restricción Legítima

  Principio que declara la necesidad de que las excepciones a los derechos fundamentales sean establecidos solamente por la Constitución Política o por la Ley vigente en cada país, de acuerdo con los principios de una sociedad democrática, en una extensión limitada y solamente cuando sea necesario para

proteger un interés legítimo de la seguridad nacional o el derecho legítimo de un ciudadano.

Se trata, como puede observarse, de un principio general aplicable en igual medida al derecho a la información y al derecho a la autodeterminación informativa; esto implica por un lado la necesaria libertad en la transmisión y acceso a la información y por otro, la necesidad de protección a la privacidad e intimidad individual frente al tratamiento de los datos personales.

El principio de restricción legítima labora de manera simbiótica con los demás principios que se estudiarán a continuación, brindando un marco general que permita establecer un equilibrio entre las necesidades de la libre circulación de los datos en general y la protección de los datos personales.

- Principio de Apertura

Principio que refleja la naturaleza transfronteriza de los flujos de datos en el mundo moderno y el ritmo acelerado de la innovación tecnológica que según Geis, Falque-Pierrotin y Suárez Crother, nos ubica en presencia "*más que de una nueva tecnología, de la construcción de un nuevo espacio social, de una nouvelle civilité (…) sinónimo de "internacionalidad del intercambio de información digital""* (Suárez Crothers, 2001).

Este principio se encarna directamente en el artículo 12 de las directrices de la OCDE sobre la protección de la intimidad y de la circulación transfronteriza de datos personales, el cual afirma que *"Debería haber una política general de apertura respecto a avances, prácticas y políticas con respecto a los datos personales. Deberían existir medios fácilmente disponibles para establecer la existencia e índole de*

*los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los datos"* (Organización para la Cooperación y el Desarrollo Económico, 1980).

Tal como lo establece la OCDE, el principio de apertura hace referencia a la necesidad de tomar en consideración el panorama cambiante ante el que se encuentran las normativas y tecnologías de protección de datos personales, con miras a asegurar su interoperabilidad y garantizar la correcta información del sujeto de datos, con miras a permitir el ejercicio de sus derechos.

## Las Etapas del Tratamiento de los Datos Personales - Principios Específicamente Involucrados

Tal como se estableció con anterioridad, la principal particularidad de la protección de datos personales es su apoyo en elementos normativos y técnicos para asegurar el derecho a la autodeterminación informativa de los sujetos de datos frente a los múltiples problemas que enfrentan en la actualidad.

La protección de datos personales es un área interdisciplinaria que se basa en el conocimiento técnico de las diversas etapas de tratamiento[70] de la información en las bases de datos, para la creación e implementación de soluciones como las técnicas y

[70] Definido por nuestra Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales como *"Cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros."* (Asamblea Legislativa de la República de Costa Rica, 2011).

estándares de seguridad de la información, los códigos de buenas prácticas corporativas, la "Privacy by Design" y por supuesto los diversos tipos de normativa aplicable.

Según Riascos Gómez, *"Morales Prats, siguiendo al iusinformático Frosini, expone que en el ciclo operativo de un sistema informático (…), se distinguen las siguientes fases: a) Fase de recogida de datos; b) Fase de tratamiento y programación de la información; c) Fase de conclusión del procesamiento de datos; y d) La transmisión de la información"*[71] (Riascos Gómez, 1999, pág. 101 vol. 2).

Desde el punto de vista de la protección de datos personales, cada etapa del tratamiento de la información por un sistema es relevante y posee sus propios principios particulares dirigidos a asegurar la solución o reparación de los daños y, revelando los contenidos de esencia, presencia y decisión a los que aludía Riascos Gómez en cada una de las fases que las conforman. Por tal motivo, a continuación se dará paso a un breve examen de las características básicas de las etapas y fases del tratamiento de los datos personales, con detalle en el estudio de los principios con ellas relacionados:

### Etapa de Recopilación de los Datos (Etapa de Input)

[71] Con miras a simplificar y dar un mayor alcance al presente estudio podrá considerarse que en términos generales las faces b) y c) señaladas por Riascos Gómez pueden ser unificadas dentro de una etapa que llamaremos "de tratamiento de los datos". A pesar de lo anterior es necesario comprender que dependiendo del tipo de aplicación brindada a los datos personales, podremos encontrar dentro de estas etapas una gran cantidad de subdivisiones.
Con miras a brindar solución a esta realidad, en la actualidad se habla sobre la necesidad de aplicar técnicas de "Privacidad por diseño", que consisten en la supervisión constante de todo proceso de tratamiento de datos (e incluso, de todo proceso de creación de aplicaciones dirigidas al tratamiento de datos) con miras a determinar los requisitos y principios específicos que logren garantizar la protección del individuo de manera completa.

La primera etapa del procedimiento o tratamiento informatizado de datos se encuentra constituida fundamentalmente por la recolección, selección y organización específica de estos.

Esta etapa es caracterizada fundamentalmente por no encontrarse completamente inscrita dentro de lo que usualmente se consideraría como tratamiento automatizado de los datos personales, dado que usualmente el proceso de recolección de datos encuentra sus inicios en el acopio manual de la información en medios físicos (a través de la plasmación de la información en medios como encuestas, entrevistas, volantes, formularios de creación de perfiles en páginas web, entre otros), lo cual usualmente requiere la labor humana para poder ser completada.

A pesar de tal particularidad, actualmente gran cantidad de los procesos de recolección, selección y organización de información personal son realizados de manera completamente automatizada, por medio de sistemas de software o hardware capaces de extrapolar y recontextualizar información a partir de las masivas bases de datos disponibles en la red actualmente[72].

*"La parte de esta fase realizada con medios y recursos de carácter humano tiene como características principales la de ser una actividad humana, especializada, personal o por regla general de carácter colectivo y multidisciplinaria, según el tipo, cantidad y calidad de información o datos recogidos. Esta parte, con todas sus ventajas o desventajas constituye una parte de la fase inicial de carácter subjetivo, bien se haya*

[72] Esto es especialmente cierto en el campo de las telecomunicaciones, cuyo funcionamiento requiere naturalmente de la generación de gran cantidad de información en la forma de datos transaccionales y de localización, cuya recolección no depende de la acción humana.

*realizado directa y personalmente o en forma indirecta con medios informáticos"* (Riascos Gómez, 1999, pág. 103 vol. 2).

A lo largo de los diversos estudios realizados sobre la materia, el Foro Económico Mundial, afirma que en la actualidad los datos personales pueden ser ofrecidos voluntariamente, observados o inferidos. Así, *"Los datos ofrecidos voluntariamente provienen directamente del individuo – fotografías, blogs, tweets, videos, comentarios, "likes", correos electrónicos y demás. Los datos observados son creados como resultado de una transacción entre un individuo y una organización – datos de localización de un teléfono móvil, transacciones de tarjetas de crédito, historial de compras en un comercio determinado, etc. Los datos inferidos, también llamados datos derivados, son el resultado del análisis, la combinación o la minería de datos, e incluyen las calificaciones crediticias, predicciones de preferencias y deseo de compra. Si los datos ofrecidos voluntariamente se sienten como una reunión social íntima, los datos observados pueden sentirse como el paparazzi que toma fotografías, mientras que los datos inferidos pueden sentirse más como un Gran Hermano que todo lo sabe y observa la cámara de seguridad"* (World Economic Forum, 2012, pág. 18).

Es en la fase de recolección de la información donde usualmente se encuentran las prohibiciones legales relacionadas con el acopio de datos sensibles; sin embargo, dadas las múltiples particularidades de la materia y la gran cantidad de formas de recolección, la correcta regulación de esta fase presenta una gran cantidad de problemas para el legislador.

Una vez recolectados los datos tiene lugar la fase de selección, dentro de la cual son identificados y separados los datos más relevantes que para los fines del

tratamiento son elegidos, para posteriormente ser compilados dentro de una base de datos durante la fase de organización.

Las diferentes fases que conforman la etapa de recopilación de los datos se relacionan con todos aquellos principios relacionados con la *"licitud, calidad, cantidad, oportunidad, proporcionalidad, compatibilidad con los fines de los datos mismos y de información"* (Riascos Gómez, 1999, pág. 108 vol. 2); sin embargo, puede señalarse que fundamentalmente se encuentra regida por los principios de pertinencia, lealtad, licitud, información y defensa de los datos especialmente protegidos; los cuales son:

- Principio de pertinencia: Requiere que la recolección de datos se limite solamente a "*los datos que sean adecuados, pertinentes y no excesivos al fin legítimo que se persigue con la creación del fichero. Cuando dejen de ser pertinentes o necesarios deben ser cancelados"* (Rodríguez Pérez, 2003, pág. 9).
- Principio de lealtad: Según Del Peso y Rodríguez Pérez, "prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos" (Rodríguez Pérez, 2003, pág. 9).
- Principio de información: Establece la obligación de *"informar al interesado al que se solicitan los datos de modo expreso, preciso e inequívoco de la existencia del fichero automatizado, la finalidad con que se recogen los datos y los destinatarios de la información; si debe responder obligatoriamente; las consecuencias de que los proporcionen o se nieguen a suministrarlos; los derechos que tienen de acceso, rectificación y cancelación; así como la identidad del responsable del*

*fichero y su dirección. Estas advertencias deben constar en los cuestionarios de recogida de datos, cuando se toman por este medio, salvo que se deduzcan claramente de la naturaleza de los datos que se piden y las circunstancias en que se recaban" (Rodríguez Pérez, 2003, pág. 9)*.

- Principio de licitud de los criterios de clasificación: El cual afirma que la clasificación y organización de los datos *"solo puede seguir criterios que no se presten a prácticas ilícitas"* (Rodríguez Pérez, 2003, pág. 10).
- Principio de defensa de los datos especialmente protegidos: Principio que fundamenta la prohibición al tratamiento de los datos sensibles o atenientes a la esfera íntima del individuo al brindar consideraciones especiales a dichos datos.

### Etapa de Tratamiento de los Datos

Etapa indudablemente relacionada con los procesos automatizados de procesamiento de datos, da inicio una vez que se cuenta con los requisitos (software y hardware) para el tratamiento de los datos anteriormente recabados. A lo largo de esta etapa se presentan fundamentalmente las fases de almacenamiento, procesamiento y seguridad o conservación de los datos.

Cada una de las fases de la presente etapa refleja un elemento necesario para el funcionamiento de un sistema informático en un marco de garantías y control sobre el procesamiento.

La primera de las fases (almacenamiento) hace referencia a la necesaria existencia dentro de cualquier sistema informático de un medio de almacenamiento (comúnmente óptico o electromagnético en la actualidad, pero que perfectamente pudiera ser fotónico, biológico o cuántico dependiendo del sistema utilizado en el futuro).

Al respecto, Riascos Gómez señala que *"El almacenamiento de datos personales constituye por tanto, una actividad tecnológica de carácter informático con soportes y medios igualmente informáticos configurada por esta parte eminentemente tecnológica (software y hardware idóneos); y otra de índole jurídica. Tecnología y derecho interactúan de forma plena en un marco de almacenamiento lícito, legítimo y ajustado a los requerimientos tecnológicos"* (Riascos Gómez, 1999, pág. 112 vol. 2).

Según el autor supracitado, este almacenamiento incluye la organización, estructuración y selección de los datos según parámetros informáticos, así como la creación de listas o índices y el asegurar la posibilidad de accesar a tales datos. En tanto la totalidad de estos procesos pueden afectar los intereses de los sujetos de datos, resulta necesario asegurar la observancia de los estándares técnicos y las disposiciones normativas vigentes en toda aplicación legal de este tipo de medios tecnológicos.

La fase de procesamiento de los datos hace referencia al uso de los datos existentes en los medios de almacenamiento con un propósito determinado. Evidentemente, dentro de esta fase se encuentra el ámbito entero de posibles aplicaciones de la información personal. La etapa de procesamiento de los datos personales analiza los datos en el contexto de la totalidad de los datos

almacenados, con miras a posibilitar la creación de nueva información significativa (tal como el determinar la calidad crediticia del usuario, sus patrones de compra, entre otros).

Finalmente, la fase de seguridad se encarga de asegurar a todas las partes interesadas que los datos no se encuentran en peligro frente a los diversos problemas relacionados con el procesamiento de la información (corrupción de los datos, violaciones de seguridad por ataques informáticos, resultados erróneos en el procesamiento por alteraciones no autorizadas a los datos, entre otros).

En este sentido, la fase de seguridad procura asegurar la confidencialidad, la integridad y la disponibilidad de la información, al asegurar que el procesamiento de los datos se dé en un contexto (sistema operativo, ubicación física, entre otros) libre de riesgos. Tal seguridad es lograda mediante el establecimiento y aplicación de técnicas de seguridad de la información que incluyan tanto medidas organizativas (destinadas a establecer procedimientos seguros de procesamiento) como medidas técnicas (destinadas a conservar la integridad de la información frente a la amenaza de su posible alteración, pérdida o robo).

Los principios aplicables a la etapa de tratamiento de los datos son principalmente los siguientes:

- Principio de exactitud: Principio que establece el *"deber que tiene el responsable del fichero de poner los medios para comprobar la exactitud y*

*puesta al día de los datos, de forma que resulten veraces, es decir, verdaderos sobre la situación real del afectado. Da lugar a los derechos de rectificación y cancelación"* (Rodríguez Pérez, 2003, pág. 10).

- Principio del consentimiento: El cual procura asegurar de manera previa al tratamiento automatizado de los datos de los cuales se cuenta con el consentimiento expreso e informado[73] por parte del sujeto de datos.
- Principio de seguridad: Relacionado con la tercera fase estudiada, dispone que *"el responsable del fichero debe adoptar las medidas técnicas y organizativas y de personal que garanticen la no alteración, pérdida y tratamiento o acceso no autorizado"* (Rodríguez Pérez, 2003, pág. 10).
- Principio de transparencia: Que establece la apertura del procesamiento al escrutinio de los interesados, con tal de comprobar su entereza y correcta aplicación de los métodos tecnológicos y organizativos necesarios para la correcta protección de los datos personales[74].
- Principio de responsabilidad: Establece la necesidad de que los controladores de datos sean los responsables de tomar las medidas

[73] Al respecto de lo cual, Barral Viñals señala que *"el consentimiento debe ser informado. La información es la clave del tratamiento derivado del uso de la red y del comercio electrónico, dada la dificultad añadida para identificar los responsables de los ficheros, la facilidad técnica para compartir información por parte de todos los agentes que intervienen en la transacción y la existencia de formas invisibles de obtenerla, a veces imprescindibles, que exigen una información ad hoc que no haga ilusorio o parcial el consentimiento del usuario"* (Barral Viñals I. , 2003, págs. 13-17).

[74] Para lo cual puede participar también un ente independiente capaz de realizar tales escrutinios y fiscalizar el proceso.

necesarias para dar efecto a los principios relevantes para la protección de datos personales.

- Principio de confidencialidad: Principio que *"obliga al responsable del fichero y a quienes intervengan en cualquier fase del tratamiento a guardar secreto profesional sobre los datos del fichero"* (Rodríguez Pérez, 2003, pág. 10).

### Etapa de Transmisión o Utilización de los Datos o Resultados (Etapa de Output)

La tercera de las etapas se relaciona con el uso final que se da a los datos una vez estos han sido procesados y con el camino que estos siguen a través de las redes una vez que han sido liberados por el procesador de datos.

La etapa de "output" se encuentra íntimamente relacionada con el derecho de información y con el habeas data en tanto es durante esta que usualmente son afectados los intereses del sujeto de datos, lo cual da lugar a su necesidad de conocer el resultado del procesamiento de los datos y de ejercer sus derechos de acceso, rectificación y cancelación de ser necesario.

Según Riascos Gómez, *"la información o datos de cualquier tipo en ésta última fase tienen por objeto la extracción, recuperación o transferencia para la simple consulta, traslado, cesión o intercambio de datos, a través de vías off line (fuera de sistemas de redes de información) u on line (vías de red de redes de información: locales o intranet's o globales o prototípicas de internet's) respectivamente, por el titular de los datos, los responsables de los ficheros o banco de datos o las personas naturales,*

*jurídicas, públicas o privadas, autorizadas por el ordenamiento jurídico o la autoridad competente para hacerlo"* (Riascos Gómez, 1999, pág. 125 vol. 2).

Se trata de una etapa cuya regulación presenta múltiples dificultades puesto que una vez que la información ha sido transmitida, resulta difícil asegurar la responsabilidad sobre esta por parte del tercero o la confidencialidad de ella. Este problema aumenta de manera exponencial en las telecomunicaciones modernas en las cuales son usuales los flujos transfronterizos de datos personales, que complican seriamente la determinación de la jurisdicción aplicable y limitan la capacidad del individuo de ejercer sus derechos.

En la etapa de output, son aplicables especialmente los siguientes principios:

- Principio de no utilización abusiva (finalidad): Según Del Peso y Rodríguez Pérez, este principio establece la obligación de que los datos objeto de tratamiento no puedan ser utilizados para fines distintos de aquellos para los que fueron recogidos (Rodríguez Pérez, 2003, pág. 11).
- Principio de publicidad: Principio que establece la necesidad de inscribir los bancos de datos ante un ente estatal con miras a asegurar el ejercicio del derecho de información, acceso, rectificación y cancelación de los interesados. Es especialmente relevante a la última etapa del tratamiento de datos personales en tanto en nuestro país el requisito de inscripción de las bases de datos se encuentra supeditado a aquellas que liberen o

comercialicen la información (lo cual usualmente sucede durante esta fase).

## *Síntesis de la Primera Sección*

Surgimiento de la Perspectiva Iusinformática: el Derecho Informático y los Orígenes de la Protección de Datos

*A lo largo de la cual se realiza un repaso de la historia de la perspectiva iusinformática y la protección de datos personales para, a continuación, examinar los fundamentos teóricos de las técnicas y herramientas iusinformáticas de protección de datos personales.*

Breve Introducción Histórica y Contextual

- El concepto de base de datos puede ser definido como *"una colección estructurada de datos mantenida en almacenamiento informático; especialmente en aquel que incorpora software para hacerla accesible en una variedad de formas"* (Beunen, 2007, pág. 21).
- Los seres humanos han almacenado información por medio de diversos sistemas a lo largo de su historia. La historia de las bases de datos automatizadas comienza en los años sesenta del siglo pasado y gracias a la gran evolución técnica experimentada estas tecnologías no solamente se tornan populares sino que garantizan tanto la resiliencia de los datos como su disponibilidad inmediata con independencia de su localización.
- Dada la necesidad de interconectar bases de datos localizadas en los diversos puntos del orbe, a partir de los años 60 se da inicio con los procesos de diseño y creación de las primeras redes informáticas, lo cual conlleva a su vez la necesidad de establecer un conjunto de sistemas y técnicas estandarizadas de seguridad de la información.
- La seguridad de la información requiere en la actualidad de una visión holística (protegiendo todas las capas de los sistemas de información); se basa en tres principios fundamentales (confidencialidad, integridad y disponibilidad) complementados por una cantidad cada vez mayor de principios adicionales establecidos por diversos entes internacionales.

- El advenimiento de las TICs requiere la superación de paradigmas y el surgimiento de nuevas disciplinas dentro del Derecho, acuerpadas bajo una nueva rama del Derecho: el Derecho Informático. Confrontados con un siempre cambiante campo de estudio, los profesionales en Derecho Informático deben adoptar una visión propia que sintetice los conocimientos técnicos especializados con la visión legal de la problemática. Es así como surge la *perspectiva iusinformática* como punto de vista holístico e interdisciplinario.
- La preocupación legal por la protección de datos personales da inicio desde el año de 1968 con la Recomendación 509 del Consejo de Europa, y a partir de este punto da inicio un proceso internacional de desarrollo legislativo clasificado comúnmente en tres generaciones, a saber:
    - Primera generación: Basada en la autorización previa de los bancos de datos en un momento histórico donde los equipos informáticos eran fácilmente localizables.
    - Segunda generación: Procura la protección de la información personal y especialmente a la protección de los datos "sensibles".
    - Tercera generación: A partir de la cual los elementos de la protección de datos comienzan a ser reconocidos como derechos ciudadanos y se comienzan a regular las técnicas de seguridad.
    - Cuarta generación: Reconocible en algunas propuestas de la actualidad que buscan superar los vacíos existentes en las leyes de tercera generación y fomentar la cooperación internacional (interoperabilidad y responsabilidad) frente al carácter transnacional de las telecomunicaciones convergentes.

## Caracterización de la Protección de Datos desde la Perspectiva Iusinformática

*A lo largo de la cual se examinan las características de la protección de datos personales desde una perspectiva iusinformática. Para ello se da inicio con la aclaración de algunos términos que comúnmente llevan a error, para a continuación*

*examinar los objetivos, sujeto, objeto y principios de estas técnicas, los cuales son finalmente expuestos en relación con las etapas del tratamiento de datos personales.*

- Usualmente se da una confusión terminológica entre *autodeterminación informativa, habeas data y protección de datos*. Con tal de disipar esta posibilidad, a lo largo de la presente investigación se considerará como:
    - Autodeterminación informativa: Derecho humano caracterizado por subsumir los principios del derecho de la intimidad dentro del marco contextual de la sociedad de la información y la comunicación, a la vez que aboga por su comunicación y coexistencia con otros derechos aparentemente contrapuestos, como el derecho a la información.
    - Habeas Data: Hace referencia a una garantía procesal que ha sido adoptada por algunos de los países que han optado por asegurar la protección de tal derecho desde el ámbito constitucional.
    - Protección de Datos: Hace referencia a un conjunto de técnicas y herramientas iusinformáticas que buscan asegurar la salvaguarda de los datos a lo largo de su necesario manejo en la sociedad de la información y la comunicación. Las instituciones jurídicas y herramientas técnicas de protección de datos personales se enfocan en estos y buscan garantizar al individuo la protección de su personalidad virtual (y consecuentemente de su autodeterminación informativa) frente a un mundo interconectado en el que la información es transmitida y tratada globalmente.
- La problemática fundamental de la protección de datos personales supera la simple búsqueda de equilibrio entre los derechos de intimidad, privacidad e información para adentrarse en la búsqueda de soluciones holísticas y equilibradas ante problemas de las más diversas índoles (tecnológicos, económicos, políticos, jurisdiccionales, entre otros).
- En la actualidad la protección de datos personales subsume dentro de sus objetivos tanto la protección del bien jurídico tutelado por el derecho a la autodeterminación informativa (la libertad individual); como la protección de todos aquellos datos que configuran y rodean la información personal (datos y

metadatos), los cuales adquieren valor por medio de su interconexión y contextualización.

- La protección ideal de los datos personales debe aceptar como necesaria la protección holística de la información individual, incluyéndose dentro de los datos personales todos aquellos cuya recopilación, tratamiento o difusión puedan afectar los intereses de su titular
- La definición del sujeto activo de la protección de datos personales ha sido un tema ampliamente discutido por las diversas fuentes doctrinarias, las cuales aún no han llegado a un acuerdo con respecto a la necesidad de extender la protección brindada por estas técnicas y herramientas iusinformáticas a las personas jurídicas.

  El sistema jurídico vigente en nuestro país reserva únicamente a las personas físicas la titularidad sobre el derecho a la autodeterminación informativa, pero esta reserva no se ve directamente traducida en las disposiciones sobre protección de datos personales, pues si bien nuestro país no admite como sujeto activo de los procesos administrativos ante PRODHAB a las personas jurídicas, nuestra ley de delitos informáticos sí las legitima para proteger sus datos personales en sede penal.

  En opinión del suscrito autor de esta investigación, esta protección bipolar se basa en la necesidad de brindar mayor protección al ser humano, para lo cual nuestra legislación contempla dos bienes jurídicos que pueden ser tutelados por la protección de datos personales: Por un lado la vía administrativa busca la protección de la libertad humana (bien jurídico tutelado del derecho humano a la autodeterminación informativa), mientras que por otro lado, nuestra legislación penal protege a la información y al dato (personal o no) como bien jurídico tutelado ante los delitos informáticos.
- Todo administrador o encargado de dar tratamiento a una base de datos puede constituirse como sujeto pasivo de las técnicas y herramientas iusinformáticas de protección de datos personales.
- Es posible identificar una gran cantidad de tipos de datos personales, dentro de los cuales se encuentran los siguientes: Datos contextuales, de contenido, de

registros gubernamentales, financieros, médicos, de actividad, del portafolio electrónico, de identidad, derivados del consumo de contenidos, relacionales, de comunicación, y de transmisión. Junto a estos, en Costa Rica la Ley No. 8968 los clasifica también como sensibles, de acceso restringido y de acceso irrestricto.

- Los principios legales generalmente aplicables al objeto de la protección de datos serán el principio de libre circulación de la información, el principio de restricción legítima y el principio de apertura.
- Es posible identificar tres etapas fundamentales en el ciclo operativo de un sistema informático, que resultan relevantes para el presente tema en tanto cada una deberá contemplar un conjunto específico de principios de la protección de datos, a saber:
    - Etapa de recopilación de los datos (input)
        - Principio de pertinencia
        - Principio de lealtad
        - Principio de información
        - Principio de licitud
        - Principio de defensa de los datos especialmente protegidos
    - Etapa de tratamiento de los datos
        - Principio de exactitud
        - Principio del consentimiento
        - Principio de seguridad
        - Principio de responsabilidad
        - Principio del deber de secreto profesional
    - Etapa de transmisión o utilización de los datos o resultados (output)
    - Principio de (no) utilización abusiva
    - Principio de publicidad

## Sección II: Telecomunicaciones Convergentes y Problemas Emergentes de la Protección de Datos

Tal como se señalara con anterioridad, desde finales del siglo diecinueve, las tecnologías de la información y la comunicación se han caracterizado por sus avances vertiginosos y su impacto en nuestra sociedad. Especialmente en el sector de las telecomunicaciones, el desarrollo tecnológico, aunado con la apertura de los mercados tuvo como resultado la popularización de las tecnologías, desplazando[75] lenta pero inevitablemente a los medios de comunicación que durante cientos de años marcaron la manera en que nos comunicábamos e informábamos (cartas, periódicos, entre otros).

En este contexto, las tecnologías de telecomunicación modernas adquieren día con día un papel más importante. A pesar de lo anterior, son realmente pocas las personas que saben de qué manera funcionan estas redes maravillosas y confían ciegamente en las tecnologías al integrarlas completamente en los aspectos más íntimos de sus vidas.

La rápida evolución de las TICs y sus efectos en la historia han demostrado que estas poseen gran potencial como herramientas que pueden ser dirigidas a fomentar el bien social, la democratización de nuestros pueblos y la inclusión de todos los individuos en un mundo de libre acceso al conocimiento. Sin embargo, pareciera que últimamente

[75] Este desplazamiento de los medios de comunicación físicos por medios electrónicos (primero analógicos y luego digitales) ha sido parte fundamental de la historia moderna y ha marcado la manera en que hoy comprendemos nuestro mundo. Así, por ejemplo, mientras que durante gran parte de la historia humana la capacidad de nuestros pueblos para comunicarse, informarse y comprender otras culturas se vio determinada por las grandes distancias que nos separaban del resto del mundo, en los últimos cien años los avances tecnológicos han ido desvaneciendo la barrera de las distancias al punto en que hoy en día consideremos usual el observar en tiempo real eventos de importancia mundial o comunicarnos internacionalmente por videoconferencias gratuitas con nuestros seres queridos por medio de nuestros teléfonos celulares.

son cada vez más comunes los casos en los cuales estas tecnologías han terminado por afectar intereses individuales, grupales y nacionales por su mal uso, incomprensión o inadecuada adopción.

Esta situación negativa ha sido especialmente perceptible desde el punto de vista de la protección de datos personales, para la cual el rápido avance de las tecnologías no ha hecho sino facilitar el acceso a infinidad de datos que anteriormente se encontraban protegidos dentro del ámbito de intimidad individual y que actualmente son tratados en cantidades exponencialmente crecientes por los más diversos actores.

Ante esta situación, es necesario reconocer la necesidad de contar con un una visión iusinformática de la protección de datos que logre adoptar perspectivas preventivas y reconozca la necesidad de popularizar el conocimiento en materia de telecomunicaciones y protección de datos, con miras a fomentar la educación de los usuarios y frente a los peligros que asechan en el mundo feliz[76] que las TICs prometen.

Precisamente por esta razón, a continuación se realizará una breve introducción a los fundamentos de las telecomunicaciones (se detallará en relación con las diferencias existentes entre los sistemas tradicionales de telecomunicaciones y las nuevas redes convergentes) para más adelante confrontar al lector con una breve introducción a la problemática que enfrenta la protección de datos personales ante estos nuevos panoramas tecnológicos.

[76] Ver (Huxley, 2007) y (Miller D. D., 2011).

## *Fundamentos de Telecomunicaciones*

La comunicación humana es un fenómeno que data de los albores de nuestra civilización. La capacidad de comunicación es una señal indiscutible de inteligencia, es una de las características que nos caracterizan como especie[77] y es responsable de la diseminación de ideas y el estímulo de las nuevas invenciones.

Según Przemyslaw & Slawomir, *"La comunicación consiste en la transferencia de información en varias formas (texto, audio, video) de un lugar a otro. Este proceso requiere por lo menos tres elementos: una fuente de información, un medio que transporte dicha información a un punto remoto y un elemento dedicado a recuperar la información transmitida" (Przemyslaw & Slawomir, 2009).*

A lo largo de nuestro largo proceso evolutivo, los seres humanos nos hemos valido de los más diversos medios y sistemas de comunicación[78] para intercambiar y preservar nuestras ideas y sentimientos, pero no fue sino hasta comienzos del siglo XIX con la invención de sistemas de comunicación basados en la manipulación de la energía[79] eléctrica, que realmente podemos encontrar ejemplos de transferencias de información a través de grandes distancias y de manera casi inmediata.

[77] Desde los primeros símbolos y pinturas rupestres creados en el Paleolítico, pasando por los petroglifos, pictogramas e ideogramas encontrados en África, Egipto y Oceanía; y culminando con la invención de la escritura, nuestra especie ha tendido siempre hacia la creación de medios de comunicación más efectivos, rápidos y duraderos.
Esta tendencia hacia la creación de nuevas y mejores formas de comunicación, (aunada con la creatividad humana y el uso de herramientas característico de los homínidos y perfeccionado por el homo sapiens) permitió a su vez que miles años atrás las primeras culturas desarrollaran medios y herramientas dirigidas al envío de señales a través de grandes distancias (como por ejemplo el uso de tambores y/o señales de humo), los cuales fueron evolucionando y dando lugar a sistemas más estables, confiables y rápidos conforme avanzó el tiempo.
[78] Definidos por Przemyslaw & Slawomir como *"conjuntos de facilidades que hacen posible la comunicación por medio de señales" (Przemyslaw & Slawomir, 2009)*.
[79] Tales como el telégrafo eléctrico y el teléfono.

El surgimiento de los sistemas de telecomunicaciones modernos implicó cambios radicales para las naciones, las cuales de la noche a la mañana (figurativamente hablando) se vieron confrontadas con la posibilidad de interconectar el mundo. Esta posibilidad fue rápidamente adoptada y de esta manera a lo largo del siglo XIX los más diversos países se dieron a la tarea de crear sus propias redes de telecomunicaciones nacionales y, posteriormente, de expandir dichas redes mediante numerosos esfuerzos de cooperación internacional[80].

Si el siglo XIX se caracterizó por marcar el nacimiento de las telecomunicaciones modernas, el siglo XX dio lugar a su evolución y perfeccionamiento. Marcado en sus inicios por el uso militar de estas tecnologías como parte de las dos primeras guerras mundiales y posteriormente por los esfuerzos de institucionalización internacional de postguerra, la primera mitad de este siglo vio nacer tecnologías como el teletipo, la radio y la televisión, las cuales cambiaron profundamente a las sociedades de la época.

Asimismo, como parte de los esfuerzos de institucionalización internacional que dieron lugar a la creación de la Organización de las Naciones Unidas, fueron formados otros entes encargados de las telecomunicaciones internacionales. El más importante de estos entes, la Unión Internacional de las Telecomunicaciones (ITU por sus siglas en inglés) absorbió en 1932 las valiosas labores realizadas por sus antecesores (especialmente de la Unión Internacional del Telégrafo) y se dedica desde esa fecha a la regulación y estandarización de las comunicaciones por radio, teléfono y telégrafo.

[80] Dirigidos fundamentalmente hacia el tendido de los primeros cables submarinos y terrestres a finales del siglo XIX gracias a la creación de instituciones como la Unión Telegráfica Internacional (1865).

En 1947 la Unión Internacional de las Telecomunicaciones es incorporada dentro de las Naciones Unidas como agencia especializada en el área, constituyéndose de esta manera en el primer esfuerzo verdaderamente internacional para la toma de decisiones en materia de telecomunicaciones, el cual contempla dentro de sus principios el de respeto al voto democrático (un voto por país independientemente de su tamaño) y que cuenta actualmente con más de 166 países miembros y con el apoyo de más de 300 agencias no gubernamentales (Katz, 1997).

La segunda mitad del siglo XX vio nacer una nueva era para las telecomunicaciones en tanto el contexto generado a raíz de la Guerra Fría fue un impresionante incentivo para el desarrollo tecnológico[81]. La constante amenaza nuclear aunada con la carrera espacial que caracterizó las décadas de los años 50 y 60 pusieron en evidencia la necesidad de las grandes potencias de contar con sistemas de telecomunicaciones que no sucumbieran ante un ataque y que pudieran llevar efectivamente señales por diversos medios aún fuera de la atmósfera terrestre. Por tal situación, en estas dos décadas fueron redoblados los esfuerzos por desarrollar y fortalecer las variadas redes de telecomunicaciones dentro del control de monopolios estatales.

Para finales de la década de los 80, sin embargo, el mundo occidental vivió un cambio en sus políticas económicas y sociales que marcaron el paso hacia la privatización de mercados y la reducción del aparato estatal. Los efectos de estas nuevas políticas no se hicieron esperar en el sector de las telecomunicaciones, en el cual se dieron cambios extraordinarios que llevaron a la popularización de las nuevas tecnologías y extraordinarios avances en los procesos de investigación y desarrollo de tecnología

[81] Así, es en esta época cuando se da la popularización de la computadora programable moderna y el desarrollo de las primeras redes de computación.

dentro del sector privado, fomentados por la libre competencia en un contexto cada vez más globalizado. En palabras de Aldana & Vallejo:

*"A finales de los años setenta y comienzos de los ochenta, el mercado de servicios de telecomunicaciones estaba integrado en su mayoría por monopolios estatales (…). La liberalización de los mercados, un movimiento general en los ochenta, abrió nuevos escenarios para los operadores de servicios de telecomunicaciones a nivel mundial. Con la liberalización, el mercado sufrió grandes cambios en muy corto tiempo. Por ejemplo, el correo electrónico (email) se convirtió en herramienta de comunicación fundamental entre personas, y la red mundial (www) se volvió indispensable para el manejo de información de empresas y trabajadores"* (Aldana J. & Vallejo C., 2010, pág. 169).

En este nuevo marco de las telecomunicaciones, el rol natural de los Estados ha pasado de ser operadores y prestadores de servicios a cumplir el papel de reguladores y garantes de la universalización de los servicios y la protección de los usuarios. Ante esta situación, el Estado se ha visto confrontado con la necesidad de encontrar maneras para regular de manera adecuada el eternamente cambiante panorama tecnológico de las telecomunicaciones, para lo cual las más de las veces debe buscar soluciones de cooperación entre los sectores público y privado, así como buscar ayuda internacional en sus esfuerzos.

Gracias a estos elementos, para la década de 1990, el mundo de las tecnologías de la Información y la Comunicación comenzó a evolucionar y a dirigirse hacia un nuevo rumbo caracterizado por importantes cambios económicos [82], industriales [83] y

[82] Neoliberalización de los mercados, las crisis económicas mundiales, la dependencia en nuevos mercados de tierras raras, el surgimiento de nuevas potencias económicas como China, etc.
[83] La implementación masiva de nuevas tecnologías de producción de bienes (como por ejemplo el uso de herramientas robóticas), la caída de grandes empresas como resultado de las crisis económicas, la

tecnológicos que redefinieron las tendencias regulatorias y difuminaron los límites tradicionales entre las diversas disciplinas involucradas en la prestación de servicios de información y telecomunicaciones[84].

Actualmente vivimos en un mundo dependiente de las telecomunicaciones, las cuales no solo damos por sentado sino que además comprendemos como sinónimo de convergencia tecnológica, pues nuestra realidad nos lleva a identificarlas con la prestación de múltiples servicios por medio de los más diversos medios de transmisión de la información.

La convergencia es una realidad innegable en las telecomunicaciones modernas y como se verá más adelante, esta ha conllevado profundos impactos en sectores ajenos al mero desarrollo tecnológico. A pesar de esta situación, la convergencia de las telecomunicaciones no es un proceso que surge del día a la mañana, sino que se da a partir de un conjunto de avances e innovaciones que afectan primero el plano tecnológico para más adelante ver multiplicado su efecto en todo el ecosistema del sector telecomunicaciones.

El proceso de evolución paralela que afecta a los diversos campos y que culmina con la convergencia de las telecomunicaciones ha sido analizado por Aldana & Vallejo, quienes dividen en su examen los fenómenos históricos y tecnológicos en tres “olas

conglomeración de grandes empresas y el uso compartido de estas de grandes fábricas de piezas electrónicas, por ejemplo.

[84] “En el sistema de las telecomunicaciones converge una serie de saberes necesarios de armonizar: los de la ingeniería, los de la comunicación social, los de la economía, los de la política, los de la gestión empresarial, los del ambiente, los del derecho, los de la educación, los de la sociología, los de los clientes y usuarios, etc.; saberes que se presentan a veces dispersos, diversos e incluso hasta contrarios. Por esto y en aras de cumplir con el interés comprometido es que se reclama una armonización de los distintos servicios involucrados para innovar la regulación para una gestión oportuna frente a los tiempos complejos” (Dromi, 2008).

tecnológicas" que en sus respectivos momentos históricos *"inducen cambios en el mercado y señalan nuevas direcciones para la regulación" (Aldana J. & Vallejo C., 2010, pág. 169)*.

Así las cosas, a continuación se examinarán brevemente las tres olas tecnológicas mencionadas por Aldana & Vallejo. Para ello deberá expandirse el análisis a partir de los postulados de las autoras y se detallarán especialmente algunos elementos técnicos que servirán para introducir al lector a algunos de los fundamentos de las telecomunicaciones modernas; todo esto con miras a facilitar la comprensión del fenómeno de las telecomunicaciones convergentes y, especialmente, de la relación de estas con los complejos fenómenos regulatorios que envuelven al sector telecomunicaciones en el mundo moderno.

## *Las Tres Olas Tecnológicas*

### La Primera Ola: De las Telecomunicaciones Analógicas a las Telecomunicaciones Digitales.

La primera ola tecnológica que debe analizarse para comprender el estado actual de las telecomunicaciones, se relaciona con el progresivo abandono de las tecnologías y redes de información y comunicación analógicas en favor de tecnologías y redes digitales puesto que estas *"mejoran el uso de los recursos y aumentan la capacidad, en ancho de banda, de las redes de comunicaciones, hacen posibles nuevos servicios y crean condiciones para la concordancia entre desarrollo tecnológico y políticas" (Aldana J. & Vallejo C., 2010, pág. 169)*

Según Aldana & Vallejo, en el sector de las telecomunicaciones, la digitalización de las telecomunicaciones fue solamente posible gracias a tres desarrollos tecnológicos: la digitalización de red, el desarrollo de tecnología de computadores y la conmutación de paquetes.

### *Digitalización de Redes*

El primer elemento debemos considerarse al estudiar las tecnologías de información y comunicación es que estas tecnologías se encuentran basadas en la transmisión de señales y datos. Esta transmisión de información puede darse de dos maneras fundamentales: por medio de señales analógicas[85] o por medio de señales digitales[86].

[85] Las señales analógicas son aquellas que representan la información mediante un conjunto de variables continuas o que "evolucionan en el tiempo en forma análoga a alguna variable física (y) Varían en forma continua entre un límite inferior y un límite superior" (Miyara, 2004, pág. 1). En otras palabras, las señales analógicas son aquellas en las cuales la información es transmitida como un conjunto de variaciones en la intensidad, temperatura, presión, tensión, mecánica, volumen, potencia o cualquier otra graduación del medio de transmisión utilizado.
En tanto se trata de señales que varían constantemente en el tiempo, podemos encontrar ejemplos de señales analógicas en toda clase de lugares. La voz humana es uno de estos ejemplos, en los cuales la información es transmitida por medio de variaciones (vibraciones) en el medio (aire) que varían a lo largo del tiempo. Este tipo de señales usualmente presentan problemas naturales como por ejemplo su vulnerabilidad ante el ruido del ambiente, el cual puede confundir al receptor e impedir la recepción correcta del mensaje.

[86] Las señales digitales son aquellas que únicamente presentan variaciones dentro de conjuntos de valores predeterminados y "bien diferenciados que se alternan en el tiempo transmitiendo información según un código previamente acordado" (Miyara, 2004, pág. 1).
La mayor parte de las señales digitales utilizadas en la actualidad solamente poseen dos estados (encendido y apagado) y gracias a ello permiten representar, transmitir o almacenar información de manera más eficiente. Así, las señales digitales poseen varias ventajas en comparación con las señales analógicas, como por ejemplo su resistencia al ruido (gracias a que los niveles utilizados para codificar la información son tan fácilmente diferenciables), la posibilidad de enviar varios flujos de información de manera paralela por el mismo medio sin que estos interfieran entre sí y la existencia de técnicas para recuperar información faltante dentro de la comunicación.

La elección del tipo de señal utilizado en una tecnología determinada resulta de especial importante al hablar de las redes de telecomunicaciones[87].

Las primeras redes de telecomunicaciones implementadas a gran escala en el ámbito mundial se encontraban basadas en el envío de señales analógicas. Esta situación implicaba grandes costos de oportunidad, dado que el envío de cantidades relativamente pequeñas de información requería de la asignación de medios dedicados de transporte, lo cual se veía traducido en mayores gastos por parte de los particulares y los operadores de servicios.

El uso de sistemas de telecomunicaciones analógicas dificultaba también las labores del Estado, el cual debía basar su regulación fundamentalmente en un enfoque de infraestructura, preocupándose básicamente por el planeamiento cuidadoso de la asignación de su espectro radioeléctrico[88] y otros medios de transmisión de información con miras a minimizar la interferencia de la información y a asegurar su capacidad de concesionar los derechos de operación de las diversas redes.

[87] Tomemos por ejemplo el sistema de telecomunicaciones más utilizado en la actualidad: el teléfono.
Inventado en 1876 por Alexander Graham Bell, el teléfono es un sistema de transmisión de información que funciona básicamente captando las vibraciones del aire (sonidos, o fuente de información) mediante un micrófono que traduce estas en vibraciones equivalentes en una señal eléctrica, la cual corre por un medio de transporte (tradicionalmente cables) hasta llegar al auricular de la contraparte (elemento dedicado a recuperar la información transmitida).
Hasta principios de los años 90, la gran mayoría de los teléfonos funcionaban mediante el envío de señales analógicas (señales eléctricas que se corresponden directamente con las características del sonido captado por el auricular) y para ello requerían de una línea de cobre dedicada únicamente a la transmisión de estas señales.
En contraposición, un sistema de telefonía basado en el envío de señales digitales (como por ejemplo los sistemas de telefonía VoIP) funciona captando las señales analógicas existentes en el ambiente (sonidos), para a continuación codificar la información de estos sonidos en una serie de números binarios (y de paso comprimirlos para que ocupen menos espacio) y finalmente enviarlos mediante el medio de transporte, para ser descodificados por parte del sistema homólogo en el destino. Esto posee una gran cantidad de beneficios, como por ejemplo la capacidad de transmitir varios flujos de información al mismo tiempo por la misma línea (que incluye por ejemplo video, texto o imágenes), e incluso una disminución en el costo de los servicios para el usuario final.

[88] Medio en el que se propagan las ondas electromagnéticas, considerado en la mayor parte de las jurisdicciones como un bien demanial.

El desarrollo de tecnologías de digitalización de redes implica cambios importantes para los sistemas de telecomunicaciones modernos al ser *"esencial en la transformación de los monopolios estatales en mercados competitivos por que introdujo arquitecturas, y estructuras de costos y conceptos nuevos acerca de la propiedad y el control de los activos" (Aldana J. & Vallejo C., 2010, pág. 169)*.

De esta manera, para el sector privado la digitalización de las redes viene a significar el surgimiento de nuevas oportunidades y servicios (tales como el envío múltiples tipos de información por un solo medio de transmisión), a la vez que conlleva a un incremento en la efectividad y la disminución de costos relacionados con el uso de las TICs.

Por otra parte, para el sector público la digitalización de las redes viene a significar un cambio radical en la manera en que es abordada la regulación de las telecomunicaciones, al verse confrontado el Estado con redes que anteriormente solamente eran utilizadas para un fin determinado y que actualmente se prestan para brindar múltiples servicios con diversos fines. Ante esta nueva realidad, el Estado se ha visto forzado a adoptar regulación que contempla tanto la infraestructura de las redes como los servicios brindados por estas.

### *Desarrollo de la Informática*

En segundo lugar, la informática moderna ha sido responsable de llevar a cabo las gigantescas labores de procesamiento de información necesarias para la transmisión de señales digitales y por ello su desarrollo ha marcado y acompañado los esfuerzos

crecientes por generar nuevos y mejores modelos de organización y operación de las redes digitales modernas, a la vez que ha implicado cambios radicales en la manera en que los usuarios finales comprenden y utilizan estas redes.

Este desarrollo se ha visto manifestado en los más diversos ámbitos y ha conllevado cambios gigantescos para las tecnologías de la información y la comunicación al permitir, por ejemplo, la posibilidad de que los usuarios cuenten con una amplia variedad de dispositivos digitales móviles de bajo costo, capaces de cumplir las tareas tradicionalmente reservadas a otros sistemas de telecomunicaciones[89], gracias a los avances en la capacidad de procesamiento y de almacenamiento de las computadoras personales y a los increíbles logros en materia de miniaturización vistos a lo largo de la última década.

El desarrollo de la informática tuvo un rol fundamental en el camino hacia la digitalización de las redes de telecomunicaciones al demostrar mediante sus avances constantes la necesidad imperiosa de aumentar la eficiencia y capacidad de las redes y las grandes ganancias que dicho esfuerzo conllevaría para todos los interesados[90].

[89] Como por ejemplo ver televisión digital o televisión IP, enviar mensajes de texto, escuchar radio por Internet, realizar llamadas convencionales, llamadas por Internet o incluso videollamadas, tener acceso a servicios de posicionamiento global, etc… A diferencia del pasado en el que el uso de tecnología analógica implicaba la necesidad de contar con un dispositivo para cada fin que se deseara cumplir, por más que las señales viajaran por los mismos medios de transporte. (Así, quien deseara ver televisión, escuchar radio y comunicarse con otras personas debía necesariamente contar con una televisión, un radio, y un teléfono (o un walkie-talkie) a pesar de que las señales de estos tres medios de comunicación se transmitieran por medio del espectro electromagnético).

[90] Al ser desarrolladas tecnologías que permitían acceder a archivos de video y realizar las videollamadas por protocolo IP dentro de redes locales de computadoras y quedar en evidencia la ineficiencia de las redes de telecomunicaciones basadas en tecnologías analógicas para brindar estos mismos servicios, por ejemplo.

### *Conmutación de Paquetes*

Tercer y último de los elementos por mencionar de la primera ola tecnológica, la conmutación de paquetes marcó un antes y un después en la historia al brindar soluciones a uno de los problemas originales de las redes de telecomunicaciones modernas: la centralización, ineficiencia y vulnerabilidad de la infraestructura de telecomunicaciones analógicas

En su libro Computer Networks, Tanenbaum (Tanenbaum & Wetherall, 2010) cuenta que pronto después de que Alexander Graham Bell patentara el teléfono en 1876, hubo una enorme demanda por su nueva invención. El mercado inicial se dirigía a la venta de pares de teléfonos y dependía del consumidor conectar un único cable entre ellos, por lo que si el dueño de un teléfono quería hablar con otras personas, este debía colgar cables y conectarse directamente con estos. De esta manera, antes del primer año de su introducción al mercado las grandes ciudades se caracterizaban por contar con gigantescas marañas de cables que conectaban estas terminales telefónicas (ver Figura 1.a).

Como primera solución a este problema, Bell ideó una red en la cual todos los teléfonos se conectarían con una estación telefónica central (ver Figura 1.b), en la cual una operadora realizaría las tareas de redirigir o conectar las llamadas de quien llamaba con el teléfono del usuario a quien se intentaba llamar (de ahí el surgimiento de los números telefónicos, pues estos simplificaron la tarea de las operadoras).

Conforme la red continuó creciendo, el problema fundamental de la centralización se hizo evidente nuevamente en tanto se hizo necesario interconectar también las diversas centrales telefónicas, para lo cual se ordenó el sistema de manera jerárquica (ver Figura 1.c); se logró de esta manera la interconexión centralizada de las redes telefónicas analógicas. Este modelo centralizado se volvió muy popular y fue utilizado alrededor del mundo durante gran parte del siglo XX; incluso fueron reemplazadas las operadoras humanas por máquinas o computadoras diseñadas para detectar los pulsos o tonos marcados por los usuarios y redirigir automáticamente sus llamadas a los números buscados.

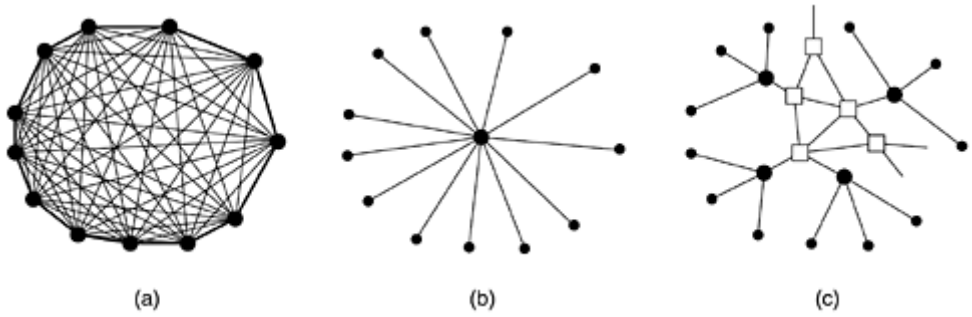



**Figura 1 (Tanenbaum & Wetherall, 2010)**[91]

Tal como se estudió con anterioridad, el desarrollo de la informática llevó a la creación de las primeras bases de datos digitales, las cuales unificaban y procesaban en un solo lugar grandes cantidades de información, y con este desarrollo surgió también la necesidad de trasladar dicha información de un lugar a otro de manera rápida, confiable y segura.

[91] (a): Ejemplo de red totalmente interconectada; (b) Ejemplo de red centralizada (red con switch central); (c) ejemplo de red centralizada con dos niveles de jerarquía.

Para lograr tal fin, las primeras redes de computadora buscaron emular el sistema interconexión total implementado originalmente en las redes telefónicas; sin embargo, conforme aumentó el número de servidores por interconectar la dificultad técnica de continuar con este modelo se hizo evidente. Asimismo, la importancia de la información transmitida por estas redes y el contexto global de la época (inicios de la Guerra Fría) llevaron a los principales interesados en la seguridad de esta información (fundamentalmente a los militares estadounidenses) a reconocer la intrínseca vulnerabilidad e ineficiencia de los sistemas centralizados, por lo que se dieron a la tarea de encontrar un sistema capaz de superar dichos obstáculos.

La respuesta a estos problemas fue encontrada por un grupo de investigadores[92] de DARPA y la corporación RAND quienes desarrollaron el concepto de conmutación de paquetes como una manera de asegurar la distribución y descentralización de las redes con miras a asegurar su resistencia a desastres (y especialmente como manera de que estas sobrevivieran incluso a conflictos nucleares).

La conmutación de paquetes propuso básicamente la creación de una red digital totalmente descentralizada en la cual la información analógica es primero digitalizada, comprimida y almacenada en el punto de origen para a continuación ser fraccionada en un conjunto de bloques de transmisión (o “paquetes”) de tamaño determinado y que son marcados individualmente con un encabezamiento que contiene la dirección del destinatario.

[92] Entre los que se encontraron Paul Rand, Ivan Sutherland, Bob Taylor, Lawrence G. Roberts, Donald Davies, Roger Scantlebury y Leonard Kleinrock (Leiner, y otros, 2009)

Estos paquetes son a continuación transmitidos a través de la red y son redirigidos individualmente (y no necesariamente de manera ordenada) por los diversos servidores o enrutadores conectados a ella, según cuenten estos con una conexión activa con el destinatario o "conozcan" de algún otro enrutador o servidor conectado al destinatario (por lo que la información será transmitida y enrutada de manera dinámica, "saltando" de enrutador a enrutador aun cuando algunas de las líneas de transmisión pudieran encontrarse caídas o dañadas).

Finalmente, una vez que los paquetes han sido recibidos por la computadora del destinatario, esta procede a "reconstruir" la información original con base en los datos encontrados en los encabezamientos de los diversos paquetes (y a solicitar se envíen nuevamente los paquetes faltantes en caso de que algunos se perdieran) y finalmente a descomprimir y a reproducir o mostrar la información al destinatario.

El modelo de transmisión de información por conmutación de paquetes no solamente fue altamente innovador, sino que fue uno de los elementos fundamentales en la creación del internet al permitir la unificación de las diversas redes de telecomunicaciones, a la vez que condujo a aumentos significativos en la eficiencia, seguridad y resistencia de las redes.

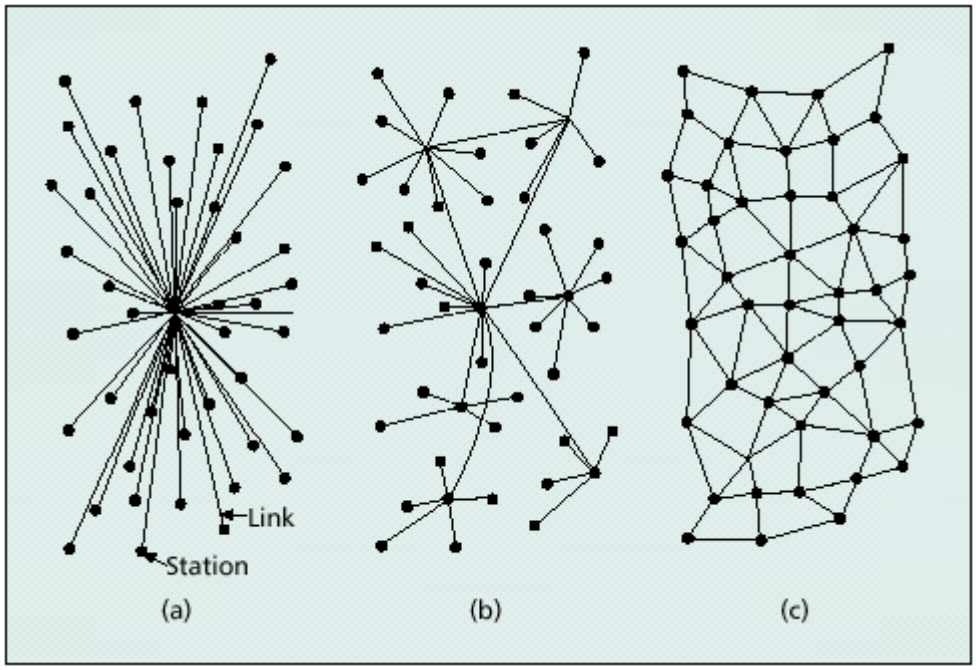



**Figura 2 (Skelsey, 2002)**[93]

El paso de las telecomunicaciones analógicas a las telecomunicaciones digitales fue un proceso largo que involucró una cantidad muchísimo mayor de elementos de los que actualmente pueden mencionarse; sin embargo, para los fines de esta investigación, es posible asegurar que la conmutación de paquetes, la digitalización de las redes y el desarrollo de la informática fueron invenciones fundamentales para la creación de las telecomunicaciones modernas y, especialmente, para el desarrollo de las telecomunicaciones convergentes.

Específicamente, el desarrollo de estas tres tecnologías permitió la unificación de la infraestructura de telecomunicaciones global y la interconexión del mundo por los más diversos medios. En otras palabras, la primera ola tecnológica logró crear las

[93] Topologías de redes: (a): Ejemplo de red centralizada conectada a un nodo central; (b): Ejemplo de red descentralizada compuesta por múltiples redes centralizadas interconectadas, lo que la hace intrínsecamente vulnerable a ataques; (c): Red descentralizada con topología totalmente distribuida conforme al modelo de conmutación de paquetes, lo cual crea una gran cantidad de nodos redundantes en el sistema que brindan seguridad a la red frente a ataques y permite el uso de múltiples tipos de conexiones para conectar los nodos (inalámbricas, fibra óptica, cableada, entre otros).

condiciones más básicas que permitirían que los sistemas de telecomunicaciones se extendieran a lo largo del orbe y lo hicieran de manera tal que hoy logren asegurar a sus usuarios la integridad, seguridad[94] e interoperabilidad de sus mensajes.

### La Segunda Ola: El Surgimiento de las Redes de Nueva Generación

Tal como se estableció anteriormente, el conjunto de avances tecnológicos logrados dentro de la primera ola tecnológica sentó las bases para la creación de redes de nueva generación (NGN)[95], capaces de brindar nuevos servicios a los usuarios finales y aumentar la capacidad de la red gracias al aumento en la eficiencia en la transmisión y la comunicación de información.

Así, la segunda ola tecnológica se presenta como un fenómeno nativo de este nuevo contexto y que aprovecha fundamentalmente los cambios tecnológicos derivados de la dinámica de la primera ola (Internet,[96] comunicaciones móviles[97] y redes de acceso de

[94] Punto aún discutible actualmente, en especial en cuanto se comprende que lograr completa seguridad en las redes de telecomunicaciones modernas resulta imposible (especialmente frente a las ya conocidas intrusiones gubernamentales).

[95] "Las NGN constituyen una red única capaz de integrar diferentes tecnologías, con arquitectura de red separada de la organización funcional (interfaces abiertas) y capacidad de inter-operar con redes tradicionales, una de sus principales ventajas" (Aldana J. & Vallejo C., 2010, pág. 170)

[96] El Internet es, sin duda alguna, uno de los mejores ejemplos que pueden encontrarse para las NGN como una red única dirigida a la integración e interoperabilidad tecnológica que se constituye actualmente como el mejor ejemplo de la convergencia de servicios.

[97] Las cuales, según Aldana & Vallejo se destacan entre las tecnologías de la segunda ola puesto "que han impulsado la telefonía y cubren una variedad de servicios, como los estándares inalámbricos y la nueva generación de tecnologías móviles. La aparición de la comunicación móvil ha influido en todos los niveles de la regulación, en particular en concesión de licencias y gestión de frecuencias; modelos de interconexión, planes de numeración y regulación de tarifas." (Aldana J. & Vallejo C., 2010, pág. 171).
Asimismo, debe recordarse que las tecnologías de telefonía móvil han pasado también por una evolución "generacional" que ha sido caracterizada según su capacidad de incorporarse al constante trasiego de datos de las Redes de Nueva Generación.

nueva generación (NGAN)[98] (Aldana J. & Vallejo C., 2010, pág. 170)[99] para generar los primeros ejemplos de convergencia tecnológica y aplicarlos de manera cada vez mayor en el sector telecomunicaciones.

El surgimiento de las *redes de nueva generación* a lo largo de esta segunda ola tecnológica, se ve acompañado también por la evolución necesaria del sector telecomunicaciones, el cual no solamente responde a la imperiosa necesidad de reducir costos unitarios por medio de la digitalización y la ampliación de sus servicios, sino que a la vez debe adaptarse al nuevo entorno tecnológico y a las constantes innovaciones del sector.

Ante esta realidad, la segunda ola tecnológica conlleva una serie de cambios que afectan directamente a todos los actores en las telecomunicaciones globales, las cuales dejan de ser concebidas como una multiplicidad de mercados separados según el tipo

---

Así, existe una primera generación de dispositivos de telefonía móvil limitados al intercambio de voz y basados totalmente en tecnología analógica, una segunda generación que incorpora la digitalización junto a sus bases analógicas y es capaz de acceder a Internet de manera rudimentaria (redes GSM e Internet WAP), una tercera generación capaz de transmitir datos a velocidades similares a las redes cableadas (3G) y nuevas generaciones como 4G y 5G que poco a poco son adoptadas en el mundo y que prometen velocidades mucho mayores y que se enfocan fundamentalmente en servicios convergentes de gama alta como lo son la telefonía sobre protocolo de Internet, las videollamadas, el teletrabajo y el streaming de video en alta definición.

[98] Caracterizadas por brindar a sus usuarios accesos más estables y rápidos a la red y comúnmente asociadas con la idea de acercar la fibra óptica al usuario final.
Sobre este punto hay que detenerse para aclarar lo siguiente: para el momento en que el internet es adoptado en gran escala (1995-2000) este era comúnmente implementado directamente sobre la red telefónica preexistente con miras a reducir costos para el Operador de servicios de Internet (ISP). De este modo, en estas redes tradicionales o de primera generación, los usuarios finales se conectaban a su ISP por medio de cables de cobre (que presentan serias limitaciones a la hora de transmitir datos).
El surgimiento de las NGAN se ve relacionado tanto con el reemplazo de la tecnología analógica por tecnología digital, como con la adopción de la necesidad de proveer al usuario final con conexiones rápidas a Internet, para lo cual los diversos ISP del mundo han debido realizar cuantiosas inversiones dirigidas a reemplazar en la medida de lo posible la tecnología basada en cables de cobre a favor de las conexiones por fibra óptica (u otras tecnologías que provean similar ancho de banda al usuario final).

[99] Ejemplos todos de tecnologías esbozadas durante la primera ola tecnológica que llegan a su madurez durante el final de la década de 1990 e inicios de la del 2000 y que al ser implementadas en masa confrontaron por primera vez al usuario con un conjunto innovador de posibles servicios y ventajas marcados cada vez más por la convergencia tecnológica.

de servicio que se brinde al usuario (radio, televisión, telefonía, mensajería, y otros) para unificarse bajo las ideas de integración e interoperabilidad de las redes de nueva generación.

Según Aldana & Vallejo, esta ola se caracteriza por el paso de *"un mercado de un solo servicio –telefonía a uno de multiservicios, que conjuga gran volumen de contenidos para diferentes tipos de usuarios y da lugar a una estructura de precios más compleja. Ya no se transan bienes simples sino sistemas de bienes, que pueden ser conjuntos de servicios o servicios por más de un período de tiempo, con estructuras de precios distintas, bien sea en mercados minoristas (usuarios finales) o en mayoristas, que incluyen al sector empresarial e institucional y a operadores de telecomunicaciones que demandan servicios por razones de conectividad. En estas circunstancias pueden coexistir distintos regímenes de regulación para diferentes tipos de servicios, de usuarios, de modalidades de negocio e incluso de tecnologías, que en principio no tienen simetría, como sucede en los cargos de interconexión fijo-móvil" (Aldana J. & Vallejo C., 2010, pág. 171)*.

De esta manera, puede culminarse el análisis de la segunda ola tecnológica comprendiéndola como la etapa que no solamente ve florecer las redes globales de información, como se les actualmente, sino que también se caracteriza por incorporar el potencial, los alcances y los efectos de las nuevas tecnologías en el quehacer cotidiano de los diversos actores del sector telecomunicaciones; se producen de esta manera cambios importantes en la organización de los mercados, el uso dado a las tecnologías por parte de los usuarios, y la manera en que todo ello es concebido por los diversos sistemas regulatorios nacionales e internacionales.

## La Tercera Ola: Nuevas Aplicaciones de las TICs

Caracterizada fundamentalmente por la innovación y la convergencia tecnológica, la tercera ola tiene lugar en el pasado cercano y la actualidad. Es un proceso incompleto aún, que no solamente genera nuevas opciones tecnológicas, sino que procura también acompañar a la constante innovación tecnológica con diversas propuestas de organización y regulación dirigidas a maximizar los beneficios de las TICs para todos los actores sociales.

Según Aldana & Vallejo *"En la tercera ola se encuentran aplicaciones de las tecnologías de la segunda ola. Estos cambios consisten en el rediseño y la racionalización de la producción, la administración y la operación de los procesos, y en la creación de nuevos productos y procesos asociados con la visión del futuro de las sociedades de la información (…) Se prevé que en esta tercera ola surgirán nuevas formas de organización y nuevos arreglos institucionales que permitan alcanzar los beneficios sociales y económicos que prometen las innovaciones. Se presume la creación de instituciones que orienten transversalmente las diferentes industrias que hoy hacen parte del sector" (Aldana J. & Vallejo C., 2010, págs. 171-172)*[100].

[100] Puede verse ejemplificada esta tercera ola en diversos sucesos relevantes al sector de las telecomunicaciones ocurridos en el pasado cercano. A modo de ejemplo a continuación se procederá a identificar los elementos mencionados por las autoras en el marco de los nuevos mercados de aplicaciones para dispositivos móviles:
Tal como mencionan Aldana y Vallejo, en esta tercera ola existen aplicaciones de las tecnologías de la segunda ola, esto es especialmente evidente en el mercado de las aplicaciones móviles, las cuales surgen en el momento en que la tecnología de telefonía móvil es adoptada a gran escala y logra incorporarse a las redes digitales de nueva generación.
En el año 2007, Apple Inc. puso en el mercado un producto característico de la segunda ola tecnológica que sin embargo había sido rediseñado de manera innovadora alrededor de una interfaz multi-táctil, nuevos productos digitales (aplicaciones móviles) y procesos abiertos (de diseño, distribución, venta, etc.) que permitían a cualquier programador incorporarse a este nuevo modelo de negocio.
Conforme las nuevas ideas implementadas por la compañía se tornaron populares, estas fueron replicadas por sus competidores con diversos grados de éxito. Esto popularizó dentro de todo el sector de tecnologías móviles el nuevo modelo de mercado que procuraba la existencia de "tiendas de

De esta manera, puede comprenderse la tercera ola tecnológica como un necesario punto de inflexión entre la innovación con otros elementos y actores[101] que asocian en ella a la convergencia tecnológica con la generación necesaria de procesos activos (y no solo reactivos) de gobernanza, dirigidos a garantizar los derechos y necesidades del sector y sus usuarios, a la vez que realicen esfuerzos por coordinar la normativa internacional relevante.

### *La Convergencia de las Telecomunicaciones*

Las tres olas tecnológicas ya estudiadas conducen en la actualidad a la llamada convergencia de las telecomunicaciones, fenómeno que como se estudiara anteriormente, surge gracias a la evolución paralela de diversos procesos históricos, sociales, políticos, económicos y (por supuesto) tecnológicos.

---

aplicaciones móviles" que permiten a cualquier persona vender sus bienes y servicios, y esto a su vez dirige a la compañía y a los programadores a un notable incremento en sus réditos.
A pesar de las múltiples y evidentes ventajas de la popularización de este nuevo modelo de negocio, no pasa mucho tiempo antes de que fueran creadas "apps" dañinas por ciertos programadores. Esta situación puso en evidencia la posibilidad de que este nuevo mercado se prestara para abusar de la confianza de sus usuarios y causarles consecuencias funestas (como violaciones a la privacidad de los usuarios, delitos informáticos, etc.).
Esta situación no tarda en generar fuertes reacciones por parte de los usuarios, las compañías y los gobiernos, y entonces que encontramos ejemplificado el "necesario surgimiento de nuevas formas de organización" y los "nuevos arreglos interinstitucionales dirigidos a orientar transversalmente las industrias" que señalan las autoras.
Las reacciones a la problemática causada por la inclusión de aplicaciones en los dispositivos móviles y los resultados de los procesos regulatorios surgidos a partir de las mismas han demostrado en los últimos años que nos encontramos ante una etapa de cambio en los procesos de toma de decisiones en la cual se torna cada vez más importante el diálogo entre las partes y la superación de los antiguos procesos de imposición de obligaciones a las compañías para entrar en los procesos de gobernanza (toma conjunta de decisiones y aplicación coordinada y transversal de estas entre los diversos actores del sector telecomunicaciones) con miras a posibilitar la visión de futuro de la sociedad de la información.
(Puede encontrarse un ejemplo de este cambio hacia la gobernanza en el proceso de múltiples interesados llevado a cabo en 2013 en EEUU con miras a asegurar la transparencia de las aplicaciones móviles (National Telecommunications & Information Administration, 2013)).

[101] Que pueden ubicarse tanto dentro como fuera del sector telecomunicaciones.

Es por esta característica de la convergencia que resulta tan difícil obtener una definición exacta del término. El tema de la convergencia tecnológica y de las telecomunicaciones se tornó especialmente popular durante los últimos años de la década de los noventas entre los estudiosos del sector telecomunicaciones, dados los movimientos de privatización e innovación en los servicios ofrecidos al público que caracterizaron la época[102].

Hablar de convergencia era equivalente durante esta época a hablar de grandes oportunidades. La palabra era utilizada indiscriminadamente[103] como una promesa que les permitía a los teóricos hablar sobre temas y tecnologías que aún no habían sido descubiertos o aplicados a gran escala (Lind, 2004) dentro del sector telecomunicaciones[104] y esta misma situación causó que este término dejara de ser utilizado tan frecuentemente, conforme la convergencia tecnológica se tornó poco a poco parte de la realidad cotidiana y comenzó a ser considerada un elemento usual (y prácticamente inseparable) de las tecnologías de la comunicación y la información.

[102] Los cuales se repiten en la Costa Rica actual, en la cual hoy en día se experimentan a la vez los fenómenos relacionados con las nuevas oportunidades de las tecnologías convergentes de telecomunicaciones con el ímpetu inicial de los mercados de telecomunicaciones recién abiertos a la competencia con operadores privados.

[103] En palabras de Lind, "Durante el curso de los 80s y 90s, el término convergencia se convirtió en una de las palabras tecno-económicas más populares en las industrias de tecnologías de la información, telecomunicaciones, internet, multimedios y de dispositivos electrónicos (el así llamado sector de las info-comunicaciones). La convergencia era utilizada para denotar casi todos los aspectos del impacto de la revolución de las tecnologías de la información. "Convergencia" podía significar cualquier cosa que tuviera que ver con nuevas aplicaciones de la computación, nuevas tecnologías relacionadas con las tecnologías de la información y los nuevos modelos de negocios. Era utilizada ampliamente con poca atención al establecimiento de una definición clara y coherente del término: el uso de las tecnologías de la información en las telecomunicaciones; la digitalización de los medios analógicos; la interconexión de computadoras por medio de redes; la televisión por cable; el uso de Internet; los servicios de banca por internet; etc. Todos estos ejemplos podían ser llamados "convergencia"" (Lind, 2004, pág. 2).

[104] Pero no limitándose al sector telecomunicaciones sino también extendiéndose a los más diversos medios de comunicación masivos en la forma de representaciones de las posibles aplicaciones de estas tecnologías en libros y películas de moda. Sobre el tema recomiendo leer (Jenkins, 2006).

A pesar de este surgimiento (y posterior declive) en la popularidad del término, actualmente se cuenta con una visión bastante clara del significado de la convergencia, la cual fue definida especialmente para el sector de las telecomunicaciones por la UIT como la *"evolución coordinada de redes que antes eran independientes hacia una uniformidad que permita el soporte común de servicios y aplicaciones" (Unión Internacional de Telecomunicaciones, 2004).* Asimismo, la Office of Communications inglesa la define como la *"tendencia a que una amplia gama de contenidos (audio, video, texto e imágenes) y servicios se distribuyan a través de distintas redes (fija, de banda ancha, infraestructura móvil, satélite, cable terrestre) a una variedad de dispositivos de consumo (pc, tv, teléfonos móviles)" (Office of Communications, 2008, pág. 61)*.

Partiendo de las definiciones anteriores y del estudio sobre las tres olas tecnológicas, puede comprenderse ahora que más allá de los meros elementos tecnológicos que posibilitaron la incorporación de múltiples tecnologías en una tendencia hacia la unificación de redes y dispositivos, la verdadera importancia de la convergencia de las telecomunicaciones se ha basado en su capacidad de superar los límites tecnológicos para afectar la sociedad de maneras totalmente imprevistas[105].

En palabras de Aldana & Vallejo, *"La convergencia pone a prueba los modelos de negocios tradicionales, genera competencia entre plataformas independientes y ejerce presión sobre los operadores tradicionales, cambia la conducta del consumidor y lo hace más activo en la demanda de servicios, y lleva a que los procesos de gestión de tecnología sean dinámicos. A su vez, estos cambios tecnológicos y de mercado ejercen presiones sobre los organismos de regulación para que se adapten al nuevo entorno. (Aldana J. & Vallejo C., 2010, pág. 173)".*

[105] Para una crítica más profunda sobre la manera en que la convergencia tecnológica ha afectado a nuestra sociedad ver (Rueda Ortiz, 2009).

Estas ideas concuerdan con la tesis sostenida por Henten, Samarajiva y Melody, quienes afirman que "*La convergencia va más allá de las innovaciones tecnológicas. Está determinada por la combinación de tendencias tecnológicas, financieras y estratégicas que pueden ser independientes de las tecnologías subyacentes" (Henten, Samarajiva, & Melody, 2003, pág. 33)".*

Siguiendo la línea marcada por los autores supracitados puede concluirse que la convergencia de las telecomunicaciones tiene, para los fines del presente estudio, una importancia fundamental en tanto pone en evidencia la vigencia imperiosa de una característica básica de la comunicación (aplicable por supuesto a las telecomunicaciones): su vinculación con la realidad humana y su capacidad de afectar directamente el comportamiento social, económico y político.

Esta característica, magnificada por las ya estudiadas interacciones entre las nuevas tecnologías y los innovadores modelos de negocios generados gracias a la convergencia, han puesto en evidencia que hoy más que nunca resulta necesario contar con reglas claras que faciliten la coordinación del sector telecomunicaciones y la protección de los usuarios de las nuevas tecnologías.

Existen ahora amenazas nunca antes vistas, como lo es la constante amenaza del cibercrimen (e incluso de la ciberguerra), que atentan directamente contra la información privada de los individuos y, por supuesto, contra los datos y metadatos que conforman su personalidad digital. Frente a esta realidad no puede caber duda de que la convergencia de las telecomunicaciones ha tenido efectos directos en los modelos de regulación nacionales e internacionales, y es precisamente en estos efectos donde seguidamente se centrará la atención.

## La Convergencia de las Telecomunicaciones y sus Efectos en los Modelos de Regulación Nacionales e Internacionales

Tal como se estableció con anterioridad, la convergencia de las telecomunicaciones ha tenido efectos directos en los fenómenos sociales, económicos, políticos [106], tecnológicos y regulatorios que conforman gran parte de nuestra realidad. Asimismo, se estableció que como parte de la tercera ola tecnológica, se ha previsto el surgimiento de nuevas instituciones dirigidas a orientar transversalmente las diversas industrias que hoy forman parte del sector telecomunicaciones.

Como resultado de estos efectos y necesidades de regulación y orientación, la evolución normativa relevante a la convergencia de las telecomunicaciones ha sufrido también una notable evolución, que ha tenido diversos niveles de impacto en los marcos normativos nacionales y en los modelos de regulación aplicables en el ámbito internacional.

### *Efectos en el Plano Nacional*

[106] Pueden encontrarse actualmente múltiples ejemplos de los efectos de la convergencia en el plano político, especialmente en tanto la popularización de las tecnologías móviles convergentes ha llevado ya al surgimiento de movimientos organizados de protesta política que han culminado incluso con el derrocamiento de regímenes dictatoriales (caso de Egipto durante la primavera árabe, ver: (Allagui & Kuebler, 2011)).

Los efectos económicos y sociales de la convergencia se tornan más evidentes en el plano nacional y es precisamente debido a esta situación que las naciones hoy se enfrentan con la necesidad de regular sus consecuencias directas (tanto positivas como negativas) en el nivel interno, a la vez que se procura adecuar el marco normativo nacional con miras a asegurar su compatibilidad con los esfuerzos realizados internacionalmente para orientar y regular a los diversos actores del sector telecomunicaciones.

A pesar de esta súbita necesidad de generar normativa específica a nuevos temas, hoy puede afirmarse que en la gran mayoría de los países estudiados la convergencia tecnológica no ha causado (¿aún?) modificaciones significativas en los procesos de génesis legislativa o de toma de decisiones regulatorias o ejecutivas.

No obstante lo anterior, desde el punto de vista de los procesos de regulación interna, es común encontrar diversos ejemplos de países que han optado por la generación de leyes específicas sobre temas anteriormente ignorados por sus diversos marcos normativos. Así, no es inusual encontrar en la actualidad países en los cuales se ha optado por regular expresamente temas como la desagregación del acceso, la separación contable, el mercado de las aplicaciones móviles, la portabilidad numérica, el acceso a internet y la brecha digital, la televisión digital, los servicios de VoIP, la neutralidad de la red, los estándares aplicables en el nivel nacional para asegurar la calidad e interoperabilidad de los servicios y por supuesto la protección de datos personales.

Por otro lado, en su intento por adecuar sus sistemas legales a las tendencias de dirección y regulación internacional, es común observar cómo las naciones del orbe han optado durante las últimas décadas, por fomentar la adopción de modelos de desarrollo compatibles con los nuevos mercados surgidos a partir de la convergencia (mediante la negociación y ratificación de tratados de libre comercio, por ejemplo) y la asignación de nuevos roles al aparato estatal (que se ha visto relegado usualmente al rol de árbitro y supervisor imparcial de los fenómenos surgidos en estos nuevos mercados).

### *Efectos en el Plano Internacional: los Modelos de Gobernanza Multilateral y el Surgimiento del Modelo de Gobernanza por Múltiples Interesados*

La convergencia de las telecomunicaciones ha tenido también efectos directos (y quizá mucho más visibles) en el plano internacional, en el cual las olas tecnológicas conllevan la creación de una serie de instituciones que realizan sus labores de dirección y regulación por medio de un modelo de gobernanza innovador (modelo de múltiples interesados) y que se contrapone en muchos sentidos al modelo tradicional (multilateral) que había caracterizado a la Unión Internacional de las Telecomunicaciones y a la gran mayoría de los esfuerzos internacionales del pasado.

Esta contraposición de modelos de regulación y gobernanza caracteriza actualmente el ámbito internacional del sector telecomunicaciones y pone en evidencia los efectos aún presentes de la tercera ola tecnológica. Entonces, puede asegurarse que para

estos dos modelos la convergencia de las telecomunicaciones ha significado múltiples cuestionamientos relevantes a dos temas fundamentales[107]: la legitimidad de las instituciones encargadas de regular las telecomunicaciones convergentes y la aplicabilidad real de las decisiones tomadas por dichas instituciones en el ámbito internacional.

Tomando en consideración que aún no se ha entrado en detalle sobre las instituciones de gobernanza internacional de las telecomunicaciones convergentes, a continuación se realizará una breve reseña de estas caracterizándolas según los modelos que representan[108], para a continuación aclarar brevemente los cuestionamientos existentes respecto a dichos modelos de gobernanza.

*La Unión Internacional de las Telecomunicaciones y el Modelo de Gobernanza Multilateral*

De acuerdo con lo estudiado durante el primer capítulo de la presente investigación, en los tiempos inmediatamente posteriores a la Segunda Guerra Mundial, los países del mundo coincidieron en la necesidad de crear un espacio de diálogo permanente, para lo cual fundaron la Organización de las Naciones Unidas. Dichos países encomendaron a esta institución con la tarea de fomentar la solución pacífica de las disputas y el fungir como un medio para coordinar esfuerzos y tomar decisiones

[107] Que pueden ser aplicados también a otras cuestiones actuales del Derecho Internacional.
[108] Entendiendo, sin embargo, que este estudio no pretende ser exhaustivo en el análisis de las características intrínsecas de los modelos de gobernanza adoptados por las instituciones internacionales analizadas

conjuntas sobre los diversos problemas que no podían ser solucionados de manera unilateral.

En este marco histórico, la evolución de las telecomunicaciones (específicamente de las telecomunicaciones analógicas) lleva a los países miembros a crear la Unión Internacional de las Telecomunicaciones, como una agencia especializada de la ONU dirigida a coordinar el uso conjunto global del espectro radioeléctrico, la promoción de la cooperación internacional en la asignación de órbitas satelitales, el mejoramiento de la infraestructura de telecomunicaciones en el Tercer Mundo y el desarrollo y coordinación de estándares técnicos internacionales.

Específicamente, la ITU se preocupa por la coordinación de tres sectores fundamentales, a saber:

- Radiocomunicaciones (ITU-R): En el que la ITU se encarga de manejar el espectro radioeléctrico y las órbitas satelitales.
- Estandarización (ITU-T): En el que la ITU es mejor conocida dada su larga historia en la creación de estándares.
- Desarrollo: En el que la ITU adopta la meta de asegurar acceso barato, sustentable y en igualdad de condiciones a las tecnologías de información y comunicación para el Tercer Mundo.

Al igual que la ONU, la ITU se basa en un sistema de diálogo multilateral que se fundamenta en asegurar que cada país miembro posea igual voz y voto en las decisiones que esta institución adopta. Estas decisiones son usualmente formuladas en

la forma de recomendaciones no vinculantes para los Estados miembros[109] y mediante un tratado internacional vinculante conocido como las "Recomendaciones Internacionales de Telecomunicaciones (ITRs)" (Unión Internacional de las Telecomunicaciones, 1989).

Considerando el tema en estudio, las recomendaciones de la ITU que se tornan relevantes serán aquellas directamente relacionadas con los procesos de estandarización relevantes a las telecomunicaciones convergentes. A pesar de ello, un estudio rápido de la historia de la institución pone en evidencia que durante una buena parte de su historia, la ITU se preocupó fundamentalmente por la regulación y coordinación del sistema telefónico tradicional internacional y no fue sino hasta los últimos años que comenzó a interesarse por la regulación de las redes de nueva generación y el surgimiento de Internet[110].

Esta situación se vio traducida directamente en la actividad de la ITU, la cual por mucho tiempo tuvo como marco de referencia vinculante solamente sus Recomendaciones Internacionales de Telecomunicaciones adoptadas en 1989[111][112]

[109] A pesar de lo cual, la naturaleza de la ITU como parte de la ONU aunada con su largo historial de trabajo en el área de las telecomunicaciones ha causado gran apoyo estatal a sus gestiones, por lo cual no es extraño encontrar países en los que las decisiones de la ITU son vinculantes o deben ser necesariamente guiar las políticas y medidas técnicas implementadas en ellos, como sucede en el caso de Costa Rica.

[110] Actualmente la ITU se encuentra en proceso de renovación de dichas Recomendaciones, para lo cual se han realizado una serie de actividades tales como la Conferencia Mundial sobre Telecomunicaciones Internacionales, para la cual se llamó a los estados miembros a generar un documento dirigido a dirigir las redes telefónicas, de televisión y de radio, y que por primera vez abarca algunos elementos relacionados directamente con internet como se verá más adelante.

[111] Y ratificadas en el 2002 por el gobierno de Costa Rica.

[112] Debe señalarse al lector también que como resultado de la Conferencia Mundial sobre Telecomunicaciones Internacionales fueron planteadas una serie de modificaciones a las Recomendaciones, las cuales entrarán en vigor en el año 2015 y de las cuales Costa Rica no es signatario.

(marcando con ello el advenimiento del movimiento internacional de privatización del sector telecomunicaciones), con tan solo 10 artículos.

A lo largo de este tratado internacional son abordados temas como la necesidad de contar con una red internacional; la implementación de servicios internacionales de telecomunicaciones; la necesidad de velar por la seguridad y la prioridad de las telecomunicaciones; la manera de realizar el cobro por estos servicios; los pasos porrealizar en caso de suspensión de servicios de telecomunicaciones; y la necesidad de diseminar información.

A pesar de la situación existente con respecto a los ITRs, la ITU-T ha generado una serie constante de estándares (no vinculantes) sobre temas como codificación de audio, imágenes fijas y video; construcción instalación y protección de cables; transmisión de datos por medio de la red telefónica; estándares de fax; redes de nueva generación para el hogar por medio de la red eléctrica; estándares para multimedia y telefonía sobre Protocolo de Internet; redes ópticas; sistemas de seguridad; y otros.

Finalmente, debe señalarse que para las labores de la ITU, y especialmente para el modelo multilateral utilizado por esta institución la convergencia de las telecomunicaciones (y especialmente la popularización del internet) ha tenido consecuencias directas al ser puestas en discusión la legitimidad de la institución para tomar decisiones pertinentes a estas tecnologías y la aplicabilidad de sus recomendaciones no vinculantes en el marco internacional (e incluso de las vinculantes por parte de aquellos países no firmantes de estas).

En cuanto a su legitimación, le son señaladas a la ITU una serie de debilidades fundamentalmente dirigidas con las deficiencias que el modelo multilateral posee, al garantizar la participación activa de los diversos interesados en los procesos de gestión y creación de nuevos ITRs. Así, por ejemplo, durante el proceso de 2012 le fue achacada a la ITU su poca disposición para hacer la información relevante al proceso de reforma de los ITRs al público, y esto a su vez puso en entredicho la legitimidad de la institución para tomar decisiones en materias relacionadas con el internet (que como se verá más adelante ha sido objeto de procesos de gobernanza participativos e inclusivos desde sus inicios).

En segundo lugar, si bien es cierto que las decisiones y recomendaciones de la ITU cuentan con mucho más peso que las de otros entes internacionales, esta encuentra problemas a la hora de asegurar la aplicación de sus recomendaciones no vinculantes en el variopinto panorama internacional[113]. Esta situación sin embargo, se ve aminorada por contar la institución con el apoyo de un sistema internacional tan bien constituido como lo es la Organización de las Naciones Unidas; no obstante, no deja de ser un aspecto relevante de ser considerado al estudiarse las ventajas de dicho sistema.

[113] El cual posee además otro problema intrínseco y relacionado con el primer punto señalado. Dada la existencia de países con diversos sistemas legales, tendencias de gobierno e intereses económicos y sociales, el sistema aplicado por la ITU cuenta con diversos problemas al permitir que las decisiones en nombre de estos países sean tomadas tan solo por representantes gubernamentales y replicadas a continuación por bloques de países que poseen intereses similares, por lo que las decisiones (adoptadas por medio de voto de mayoría) pueden no dirigirse necesariamente a garantizar los mejores intereses de la generalidad.

*La Gobernanza de Internet y el Modelo de Múltiples Interesados*

El internet, tal como fue estudiado con anterioridad, es una red descentralizada de redes de computadoras interconectadas cuya importancia social, económica y política crece exponencialmente. Sin profundizar en aspectos técnicos, puede afirmarse que el internet presenta un problema para todo esfuerzo regulatorio, tal como lo establece Suñé Llinás:

*"La regulación jurídica de Internet, por ejemplo, plantea problemas globales, que requieren de soluciones globales. Las grandes multinacionales del sector teleinformático, que lo dominan casi por completo, no pueden –ni quieren- adaptarse a regulaciones estatales injustificadamente diversas y dispersas, cuando el mercado no es nacional, sino global. Una buena legislación estatal en materia, por ejemplo, de protección de datos personales, puede verse seriamente limitada en su eficacia, si en otros Estados no existen medidas legislativas sobre la cuestión, o son muy tenues, puesto que la información no conoce fronteras"* (Suñé Llinás, 2006, pág. 314).

El carácter descentralizado del internet resulta problemático dado que todo esfuerzo regulatorio que pretenda ser eficaz debe tomar en consideración que se encuentra ante un objeto intangible fundamentalmente extraterritorial, sobre el cual realmente ningún país, individuo o corporación puede alegar titularidad exclusiva [114] . Efectivamente, la red de redes es propiedad tanto de las grandes corporaciones que prestan sus servicios e infraestructura, como de los gobiernos, que facilitan su adopción y brindan sus recursos, y de los usuarios finales (todos y cada uno de

[114] Sobre el tema se hace referencia con mayor detenimiento más adelante, pero como resumen del tema se sugiere la consulta de la siguiente fuente en línea: http://panos.org.uk/wp-content/files/2011/03/who_rules_internetg9wElU.pdf.

nosotros) que por el mero hecho de utilizar y conectarse al internet alimentan y forman parte del conjunto de los datos y direcciones que lo conforman.

Ante este panorama, resulta evidente la necesidad de identificar al ente encargado de gobernar al internet y de establecer las reglas que lo rigen; sin embargo, la inexistencia de titularidad exclusiva sobre este, aunado con la inmensa cantidad de personas, empresas, gobiernos y entes interesados en él, implica que ningún gobierno pueda realmente pretender gobernarlo.

Con motivo de esta dificultad intrínseca, los primeros años de la historia del internet vieron nacer también un innovador experimento, en relación con el cual los diversos actores involucrados el desarrollo y popularización de la red de redes comenzaron a organizarse y a idear por sí mismos la manera más adecuada de gestionar los recursos escasos con los que se contaban y dirigirse a garantizar el respeto de un conjunto determinado de principios que consideraban fundamentales.

A pesar de las múltiples dificultades existentes, este experimento por generar un sistema de dirección propio al contexto único del internet prosperó. A través del apoyo inicialmente brindado por algunos gobiernos, individuos y empresas pioneras (y la posterior inclusión de un gran número de actores y representantes del resto del mundo)[115] poco a poco fue generado un modelo basado en la cooperación y el diálogo de los múltiples actores interesados[116].

[115] Con miras a comprender correctamente la manera en la que el internet es manejado actualmente debe comprenderse que en sus inicios (en territorio estadounidense), ARPANET era manejado en su totalidad por el Departamento de Defensa de los Estados Unidos de América, sin embargo conforme el fenómeno de la interconexión de redes comenzó a tornarse un fenómeno global, el control estadounidense fue disminuyendo y fueron creadas muchas de las instituciones actualmente

Es de esta manera como comienza la evolución de este nuevo modelo, el cual hacía propios los principios de apertura y la inclusión en equidad de nuevos actores, con miras a garantizar su universalidad y aplicabilidad internacional. Para ello, este nuevo modelo procuró asegurar la participación activa de sus actores en la toma de decisiones mediante un sistema de "abajo hacia arriba" el cual procuraba que todas las decisiones adoptadas fueran basadas en el consenso y no en la imposición.

El marcado éxito de este movimiento pronto llevó al reconocimiento internacional de este sistema como una nueva forma de "gobernanza", constituida en el marco del Internet como una forma válida de organización y dirección de carácter fundamentalmente técnica, que procuraba ser independiente de los conceptos tradicionales de soberanía y jurisdicción relacionados con el Derecho Internacional Público y basado principalmente en los nexos contractuales existentes entre los diversos actores.

Finalmente, este modelo fue reconocido mediante el término *"gobernanza de internet"* durante las Cumbres Mundiales sobre la Sociedad de la Información (CMSI) organizadas por la ITU en Ginebra (2003) y Túnez (2005). Y es también en este contexto que es definido como *"el desarrollo y aplicación por parte de los Gobiernos, el sector privado y la sociedad civil, en sus respectivos papeles, de principios compartidos, normas, reglas, procesos de toma de decisión y programas que conforman la evolución y uso de Internet"* (Organización de las Naciones Unidas, 2005).

encargadas de coordinar los procesos de Gobernanza de Internet, las cuales poco a poco adoptaron también un carácter mucho más internacional.

[116] Dentro de los que pueden encontrarse representantes gubernamentales, dirigentes de la industria e incluso miembros de la sociedad civil y la academia, todos cooperando en un marco de igualdad de oportunidades.

Entrando un poco en detalle sobre el funcionamiento del modelo de gobernanza de internet, debe establecerse inicialmente que este se basa, al igual que en el caso del sistema multilateral, en la existencia de una serie de instituciones (que en este caso son organizaciones no gubernamentales) las cuales cumplen diversos roles dentro del ecosistema de internet.

De esta manera, la actual gobernanza de internet es coordinada gracias a la cooperación de las siguientes organizaciones:

1) La Corporación de Internet para la Asignación de Nombres y Números (ICANN): Encargada de asignar bloques de direcciones del protocolo de internet alrededor del mundo y coordinar el sistema de nombres de dominio.

2) La Sociedad del Internet, organización no gubernamental dirigida a la formación de capacidad dentro de la sociedad civil y de facilitar la inclusión de los diversos actores dentro de los procesos de gobernanza de internet (lo cual incluye también labores de mediación y coordinación con los gobiernos y sus representantes). Asimismo, está dentro de sus responsabilidades coordinar discusiones sobre todos aquellos temas que pudieran verse afectados o afectar directa o indirectamente al internet, como por ejemplo: cibercrimen, multilingüismo, protección de datos y privacidad, propiedad intelectual, comercio electrónico, métodos de seguridad y estabilidad del internet, entre otros.

3) Los diversos entes dirigidos a la estandarización técnica (y abierta) de las tecnologías de la información y la comunicación, como lo son el World Wide

Web Consortium (W3C), la Organización Internacional para la Estandarización (ISO) la Internet Engineering Task Force (IETF), la Internet Research Task Force (IRTF) y otros.

Las labores de gobernanza de internet llevadas a cabo por todas estas organizaciones son logradas gracias a su carácter inclusivo y abierto. Las decisiones de los diversos entes (específicamente de los entes estandarizadores, y quizá con la excepción de las decisiones concernientes al sistema de DNS manejado por ICANN) no son por lo general vinculantes para los diversos interesados involucrados en el ecosistema de internet.

No obstante lo anterior, las decisiones generadas en los procesos de gobernanza de internet cuentan con la particularidad de ser, por lo general, respetadas e implementadas a gran escala por los actores (y especialmente la industria y los gobiernos) debido a que todos ellos fueron parte de los procesos que llevaron a la toma de dichas decisiones y las cuales solamente pudieron ser adoptadas mediante su consenso.

A pesar de esta situación de aparente cordialidad, el sistema de gobernanza por múltiples interesados implementado en la actualidad, en la gobernanza de internet se enfrenta también con los problemas de legitimidad y aplicabilidad que aquejan al sistema multilateral.

En materia de legitimidad, la gobernanza de internet se enfrenta en primer lugar con el problema de hacer realmente inclusiva y democrática la participación de todos los sectores de la sociedad dentro de sus procesos. En un mundo ideal en el que sus

postulados fundamentales pudieran ser efectivamente implementados, la gobernanza de internet buscaría asegurar la participación de todos los usuarios finales, compañías (independientemente de su tamaño) y Estados, en los procesos de toma de decisiones (por medio de una especie de sistema de democracia participativa perfecto).

Evidentemente, en el mundo actual, asegurar una participación tan amplia resulta imposible, y por ello las diversas organizaciones relacionadas con la gobernanza han debido centrar sus esfuerzos en facilitar el acceso a la información por medio de la red y asegurar la asistencia de una cantidad (cada vez mayor) de individuos y representantes de instituciones públicas y privadas a sus reuniones.

Lamentablemente, esta solución no ha sido capaz de solventar el problema de asegurar que en las discusiones de gobernanza de internet se encuentren representadas correctamente la totalidad de las posiciones e intereses individuales, y el hecho de que solamente unos cuantos individuos (no elegidos democráticamente para representar a sus pueblos) puedan participar en dichas discusiones no han hecho sino disminuir la legitimidad de las instituciones frente a los ojos del público.

En segundo lugar, la legitimidad de los procesos e instituciones de gobernanza de internet se ha visto socavada por la cada vez mayor contraposición existente entre los entes encargados de coordinar estos esfuerzos con los entes multilaterales ya estudiados (ONU y ITU). Dicha contraposición (que otrora fuera prácticamente inexistente, dado el énfasis de la ITU en la regulación de las redes tradicionales), ha crecido y se ha hecho evidente en los últimos años, conforme ha crecido el interés nacional e internacional por regular los fenómenos surgidos en internet.

Finalmente, la legitimidad de los entes encargados de coordinar los procesos de gobernanza de internet se ha visto afectada por la relación y dependencia que muchos de estos aún guardan con el gobierno estadounidense. Dicha situación ha generado malestar en el plano internacional, conforme ha pasado el tiempo y se han dado situaciones en las cuales el gobierno de EEUU ha utilizado su relación con estos entes para expandir su jurisdicción a otros países[117].

En cuanto a los problemas de aplicabilidad de sus decisiones en el plano internacional, las limitaciones del sistema de múltiples interesados deberían resultar evidentes, con tan solo recordar que, en términos generales, las decisiones a las que llegan estas organizaciones no poseen carácter vinculante para sus miembros, por lo cual resulta imposible obligar efectivamente a que ningún actor del ecosistema de internet las adopte.

Ahora, si bien es cierto que, como se dijo anteriormente el problema de la aplicación no resulta necesariamente problemático puesto que se cuenta en términos generales con consenso en la toma de decisiones de carácter técnico (como por ejemplo la formación de estándares abiertos), los límites de aplicabilidad de las decisiones continúan siendo problemáticos. En el sistema actual de gobernanza por múltiples interesados, no existe aún manera de extender las discusiones a temas de fondo (como por ejemplo la necesidad de asegurar la protección de la privacidad y la protección de los datos de los usuarios) y lograr llegar a acuerdos vinculantes por parte

[117] Tal como sucedió en el caso del cierre de Megaupload por piratería (Anderson, 2012) y especialmente en el caso de Bodog.com (Geist, 2012), en el cual el gobierno estadounidense afirmó tener jurisdicción sobre todos las páginas registradas bajo los nombres de dominio genéricos de primer nivel ".com", ".org." y ".net".

de los diversos actores[118]; es por ello que hoy estos temas deben ser abordados en cumbres impulsadas por la ITU (como lo son la Cumbre Mundial de Tecnologías de la Información y el Foro de Gobernanza de Internet).

Este punto coincide nuevamente con el tema de la presente investigación. Para la protección de datos personales la convergencia de las telecomunicaciones ha puesto en evidencia que en la actualidad resulta imposible escindir los procesos de regulación nacional de las decisiones tomadas en el marco internacional. Asimismo, ha demostrado que todo esfuerzo por proteger datos personales en las telecomunicaciones modernas resultará vano de no contarse también con una adecuada protección de los datos que son transmitidos por internet[119].

Frente a esta realidad, en consideración del suscrito autor de esta investigación, resulta prudente concluir este apartado recordando las palabras de Suñé Llinás, quien afirmara que *"La Protección de Datos Personales en Internet está condicionada por el carácter básicamente inseguro de La Red, así como por su calidad de red global. La inseguridad técnica de los niveles básicos de Internet propicia los abusos en la captación de datos personales, en el que están interesadas importantes empresas multinacionales, que son precisamente las que han de desarrollar los productos, hardware y software que permiten operar en Internet. Asimismo Estados de gran peso específico tienen interés en controlar la información que circula por Internet, y de hecho lo hacen"* (Suñé Llinás, 2006, pág. 320).

[118] Problema que se evidencia también en el sistema multilateral pero que en términos generales es superado en tanto se cuenta con una cantidad menor de actores (representantes de países miembros) en capacidad de tomar decisiones a nombre de su país, por lo cual se pasa a hablar de falta de voluntad política y no de problemas por legitimidad o por capacidad de representación.
[119] Por lo que de pretenderse una solución real al problema, este deberá ser abordado necesariamente tanto en el marco del sistema multilateral como en el sistema de gobernanza por múltiples interesados.

Tal como se estudiará a lo largo del siguiente apartado, las palabras de Suñé Llinás continúan siendo válidas en la actualidad, pues, junto con las grandes posibilidades, la convergencia de las telecomunicaciones trajo también una serie de problemas emergentes que afectan específicamente a la protección de datos personales y que son objeto de los esfuerzos regulatorios (nacionales e internacionales) ya estudiados.

## *Problemas Emergentes de la Protección de Datos Frente a la Convergencia de las Telecomunicaciones*

De conformidad con lo estudiado a lo largo de la sección anterior, la protección de datos personales cuenta con características especiales, que la delimitan desde una perspectiva iusinformática como materia, en sus esfuerzos por cumplir su objetivo principal: proteger los datos personales y el derecho de autodeterminación informativa frente a todas aquellas situaciones capaces de afectar negativamente los intereses de sus titulares.

El reconocimiento de este objetivo como fundamental para la protección de datos personales ha dado lugar a la formulación de las teorías y principios anteriormente estudiados, los cuales deben, idealmente, ser aplicados en todas las fases del tratamiento de datos personales por medios manuales o automatizados, independientemente de la naturaleza del ente encargado de realizar tal tratamiento.

Lastimosamente, la aplicación práctica de la protección de datos personales se ha visto siempre confrontada con un espinoso panorama, conformado por las dificultades

intrínsecas de llevar a la realidad un proyecto tan ambicioso como lo es la protección de la totalidad de los datos y metadatos concernientes a un individuo. Este panorama ha sido complicado aún más por el surgimiento del internet y la rápida evolución y convergencia de todas las tecnologías con él relacionadas.

Actualmente, la protección de datos personales se enfrenta a un amplio grupo de problemas emergentes debidos, según Stefano Rodotà, a tres razones fundamentales: 1) la reducción de garantías y el cambio de los criterios de referencia a partir de los hechos ocurridos el 11 de septiembre de 2001; 2) la extensión de esta tendencia de reducción de garantías a sectores no relacionados que intentan sacar ventajas de la mutación del clima general; y 3) los continuos y crecientes instrumentos de clasificación, selección y control de las personas ofrecidos por las nuevas tecnologías que determinan una situación de deriva tecnológica ante las cuales ni las autoridades nacionales ni las internacionales logran responder adecuadamente (Rodotà, 2006, pág. 55).

Como consecuencia de esta cadena de acontecimientos, Rodotà considera que se ha producido una erosión de los principios sobre los que se ha basado el sistema de protección de datos. Así, actualmente es común observar cómo el principio de finalidad y el relativo a la separación de los datos trazados por sujetos públicos y privados, se carcomen al favorecer el criterio de multifuncionalidad[120] y las lógicas de la reutilización y de la interconexión con los argumentos de la eficiencia y la economicidad (Rodotà, 2006, pág. 55). Asimismo, señala el autor tres tendencias convergentes que restringen la protección de datos: las tendencias hacia la totalidad,

[120] Que afirma la posibilidad de utilizar los datos para fines diversos de aquel por el que fueron recogidos y busca incluso facultar a nuevos sujetos para realizar tal tratamiento.

la permanencia y la disponibilidad de las informaciones recogidas, y con ellas el abandono de los principios de proporcionalidad, pertinencia, finalidad y necesidad.

A partir de este marco contextual, se procederá a continuación a examinar algunos de los problemas emergentes más relevantes para la protección de datos personales, a lo largo de los cuales se intentará identificar concordancias con el abandono de los principios fundamentales de la protección de datos al que hace referencia Rodotà.

## Proliferación de Cookies

Conforme las tecnologías de la información y la comunicación se han vuelto más avanzadas, han tomado prevalencia los mecanismos dirigidos al rastreo sin consentimiento del comportamiento individual. Esta afirmación es especialmente relevante al examinar la evolución del internet, en el cual la cantidad de datos recopilables se ha expandido exponencialmente a la vez que se han puesto a disposición de entes privados y públicos las herramientas para obtener tales datos.

En el caso del internet, las herramientas de recolección de información sobre el comportamiento difieren ampliamente de las utilizadas tradicionalmente; no se está ya ante un sujeto que espía a través de ventanas y cerraduras de puertas, sino que son utilizados medios casi imperceptibles para el usuario común, dado que han sido diseñados para nunca desvelar su presencia.

Este es el caso de las "*cookies",* las cuales son definidas por Mayer-Schönberger y Mosing, como *"piezas de información generadas por un servidor Web y almacenadas en la*

*computadora del usuario, listas para accesos futuros. Las Cookies se encuentran insertas dentro de la información HTML*[121] *que fluye entre la computadora del usuario y los servidores. Las cookies fueron implementadas para permitir customización del lado del usuario de la información web"* (Mosing, 2003, pág. 4), en su sentido más simple, las cookies no son más que pequeños documentos de textos inyectados por los servidores web en la memoria de las computadoras de sus usuarios, para almacenar información sobre el usuario y su equipo, la cual más adelante pueda ser recuperada.

Según Mossig, las cookies basan su funcionamiento un simple proceso; consistente en una primera etapa, en la cual la cookie es almacenada por el servidor en la computadora del usuario en un archivo especial llamado lista de cookies; y una segunda etapa, en la cual el servidor obtiene acceso a su Cookie cuandoquiera que el usuario se conecte a él.

Según Zimmerman, *"Las Cookies pueden afectar la privacidad de un usuario de dos maneras primarias. Primeramente, las Cookies son almacenadas en el disco duro del usuario y pueden ser accesadas en una fecha posterior. Una vez realizado el acceso las Cookies mostrarán una lista detallada de cada sitio web que ha sido visitado por esa computadora dentro de un lapso temporal relevante. Más aún, el texto del archivo de Cookie puede contener información personal sobre el usuario tal como su password, dirección de correo electrónico o cualquier otra información brindada por el usuario dentro de la página en cuestión. (…) La segunda manera en la que las Cookies pueden afectar la privacidad se basa en el hecho de que los servidores de las páginas web que envían las Cookies también reciben la información almacenada en esa Cookie particular cuando el usuario visita nuevamente la misma página*

[121] Hypertext Markup Language, sistema estandarizado para describir la estructura y el contenido de archivo de texto que permite a su vez anexar "objetos" a dichos archivos, tales como imágenes, videos, música, etc. Se trata del principal lenguaje de programación utilizado para el desarrollo de páginas de Internet, el cual ha evolucionado a lo largo de sus diversas versiones.

*web. Usando esta cookie las páginas son capaces de rastrear de que sitio fue referido el usuario, los links en los que el mismo hizo click, si realizó alguna compra y toda información personal brindada por el interesado"* (Zimmerman, 2001, págs. 442-443).

Si bien en sus inicios la utilización de cookies procuraba simplemente brindar al usuario una experiencia más amena y personalizada en las diversas páginas web que este visitaba, rápidamente este sistema llamó la atención de las grandes compañías de publicidad en internet, quienes encontraron en ellas una nueva fuente de divisas: la venta de publicidad personalizada.

En la actualidad las cookies en el internet *"se han multiplicado a una velocidad que impresionaría a los epidemiólogos"* (Riofrio, 2013, pág. 1), al punto de que se ha llegado a considerarlas como parte ineludible de la navegación por la red de redes. Gracias al desinterés de usuarios y entes reguladores por igual, las cookies en la actualidad son utilizadas fundamentalmente con el fin de establecer patrones de comportamiento individual, los cuales posteriormente son monetizados por compañías especializadas en el negocio (y no necesariamente relacionadas con el proveedor de la página web a la que accedió el usuario) y vendidos al mejor postor.

La problemática del uso de cookies se relaciona hoy en día, principalmente con la inconsciencia entre los usuarios sobre la situación. En tanto la mayor parte de los programas y páginas web disponibles no informan al usuario sobre el uso de cookies o los fines del rastreo, los usuarios desconocen el riesgo en que se encuentra y, por supuesto, ignoran la existencia de métodos de protección contra este.

Esta situación ha sido aludida por los diversos sistemas legales de maneras muy variadas; dentro de ellos, es digno de mención el sistema Europeo por contar con disposiciones específicas sobre el tema en la Directiva 2003/58/EC sobre privacidad y comunicaciones electrónicas. Asimismo, en el ámbito técnico se han propuesto diversos estándares dirigidos a solventar la situación. Dentro de estas propuestas puede mencionarse, por su actual popularidad el estándar llamado "Do Not Track", el cual añade a toda la información que sale de la computadora del usuario una indicación expresa de que este no desea ser rastreado (Mayer, Narayanan, & Stamm, 2011).

A pesar de tales esfuerzos, el problema aún continúa sin respuesta definitiva. Las propuestas normativas realizadas no han sido muy populares (han encontrado oposición marcada por parte de las compañías cuyos modelos de negocio dependen de las cookies) por implicar la realización de una serie de advertencias al usuario que aumentan la cantidad de trabajo que este debe realizar y la dificultad de lectura de los contratos y términos de servicio. Asimismo, se debe resaltar que es poca la experiencia con que a la fecha se cuenta en este tema, dada la limitada cantidad de países que han creado legislación específica al respecto[122].

Igual panorama confronta a las propuestas técnicas presentadas, las cuales usualmente no logran configurarse como estándares vinculantes para la industria, en

[122] Por otra parte, resulta importante también recordar que la tecnología de rastreo por medio de cookies, al igual que la totalidad de los medios tecnológicos de los que nos valdremos como ejemplos a lo largo de la presente investigación se encuentran en constante evolución, por lo que resulta necesario considerar su avance y cambio acelerado dentro de cualquier propuesta normativa que se procure realizar. Específicamente en el tema de las Cookies, ya algunos medios han señalado una tendencia creciente hacia su desaparición a favor de métodos nuevos mediante los cuales las grandes empresas (Google, Microsoft, Facebook, y otros) procuran superar su dependencia en terceras partes y las limitaciones intrínsecas de la tecnología de Cookies (poca compatibilidad con dispositivos móviles por ejemplo) y crear sus propios sistemas de rastreo y monitoreo de usuarios (Dwoskin, 2013).

tanto no cuentan con el apoyo de las grandes compañías. Este es el caso de "Do Not Track", la cual a la fecha no ha sido adoptada por la Internet Engineering Task Force (ente global encargado de la creación de estándares para internet) como estándar oficial. Asimismo, "Do Not Track" se enfrenta al problema que representa la inexistencia de apoyo normativo vinculante a la decisión del usuario de no ser rastreado, por lo que sus disposiciones se tornan vacuas frente a la realidad.

A partir del estudio realizado, puedes concluirse que la problemática en torno de las cookies se relaciona íntimamente con la tesis del abandono de los principios de la protección de datos que sostiene Rodotá. En el marco actual de manejo de cookies, resulta sumamente difícil considerar que sean aplicados los principios de pertinencia, lealtad, información, licitud y de defensa de los datos especialmente protegidos, en un sistema que se caracteriza por su secretismo para con el usuario, y que se dedica abiertamente al uso comercial de los datos recabados.

### Elaboración de Perfiles y Redes Sociales

En íntima relación con el tema anteriormente tratado, el surgimiento de las redes sociales ha implicado un cambio completo en el paradigma de los sistemas de protección de datos personales, al involucrar activamente al sujeto de datos en el proceso de recopilación de la información y de generación de perfiles personales.

Tradicionalmente, la información personal era recopilada, tratada y transmitida a gran escala solamente por entes externos al individuo común. Efectivamente, con base en

los estudios realizados sobre la visión tradicional del derecho a la intimidad y especialmente la manera en que fue desarrollado el derecho a la privacidad en el sistema anglosajón, con excepción de algunos individuos considerados "de interés público" (celebridades, políticos y otros) el común de los ciudadanos de una nación solamente reportaban con regularidad sus datos personales a las bases de datos gubernamentales (censo, seguro social, ministerio de trabajo, entre otros) con miras a obtener o formar parte de los servicios ofrecidos por el Gobierno.

El surgimiento del internet "civil", aunado con el avance en la miniaturización y la reducción de precio, relacionada con el surgimiento de los sistemas informáticos personales, condujo a que ya en la década de 1990, la tendencia de reportar regularmente los datos solamente a entes gubernamentales comenzara a cambiar. Tal como se estudió anteriormente, el surgimiento de estos sistemas permitió tanto a la empresa privada como al individuo común, la creación de bases de datos privadas.

Asimismo, es durante la década de 1990 que comienza a popularizarse la creación de páginas web personales, en las cuales los individuos eran capaces de publicar al mundo todo aquello que quisieran, sin tener que pasar por el control de intermediarios. Esto llevó a muchos a publicar por este medio tanto sus creaciones (libros, revistas, arte y otros) como información relacionada con su persona (currículum vitae, correos electrónicos y físicos para facilitar ser contactados, entre otros aspectos).

La etapa tardía de los años 90 trajo consigo la popularización de la web 2.0, en la cual era posible crear fácilmente páginas con mayor contenido multimedia, las cuales eran capaces de ser modificadas por los usuarios con facilidad. Tal situación desencadenó el

inicio de nuevos proyectos de emprendedores, dirigidos a crear “la nueva gran cosa” en el internet y como resultado de estos proyectos fueron creadas las primeras plataformas de servicio de creación de redes sociales.

Las primeras redes sociales consistían usualmente en una página web que permitía a sus usuarios la capacidad de alterar y guardar una página en sus servidores, dirigida a representar al usuario en la red, por medio de la creación de un perfil controlado por él. Asimismo, estas páginas permitían al usuario señalar su pertenencia a ciertos grupos (como por ejemplo grupos de debates, o grupos generacionales académicos).

Ya para el nuevo milenio, las redes sociales habían adquirido completa popularidad y se diferenciaban de la competencia usualmente brindando mayor capacidad de personalización de su perfil individual (Friendster, Hi5 y MySpace). Todas estas páginas se caracterizaban, sin embargo, por un elemento fundamental: el contenido de la página era provisto en su totalidad por el usuario, quien por lo general basaba los contenidos de su página en información relacionada con su vida real.

El éxito de estas páginas contribuyó finalmente al surgimiento de nuevas iniciativas dirigidas a requerir y brindar información personal más relevante a sus usuarios para el cumplimiento de diversos fines. De esta manera, en el año 2003 abrió sus puertas LinkedIn, una página web dirigida a conectar digitalmente a profesionales, para lo cual son requeridos usualmente datos fidedignos sobre la historia personal de sus usuarios. Y en el 2005 es lanzada Facebook, actualmente la red social más grande del mundo, caracterizada por contar con información sobre una gigantesca cantidad de individuos.

En la actualidad es posible definir el concepto de red social (en línea) como aquel *"servicio que se enfoca en la creación y verificación de redes sociales en línea para creaciones de personas que comparten intereses y actividades, o que se interesan en explorar los intereses y actividades de otros, para lo que requiere del uso de software"* (International Working Group on Data Protection in Telecommunications, 2008).

*"En el contexto de las redes sociales, los usuarios eligen divulgar información personal con miras a "hacer un perfil" de sí mismos y para participar en la comunidad de usuarios. Ellos publican una "identidad personal" al publicar selectivamente información personal en sus perfiles. Esta identidad digital es su representación en el mundo en línea y para algunos usuarios una "manifestación de (…) personalidad," La conexión entre la persona en línea y la realidad fuera de línea del individuo es, usualmente, un aspecto importante de la mayor parte de las redes sociales. Esto es obvio especialmente cuando los usuarios participan con sus nombres verdaderos y publican fotografías de sí mismos. El sentido de "encontrarse conectado", usualmente con una comunidad fuera de línea o con una nueva comunidad en línea, creada por una red social, es parte de su éxito y parte del reto desde la perspectiva de la privacidad"* (Kartzi, 2008, pág. 7).

Tal como lo manifiesta Kartzi, el éxito de las redes sociales se basa fundamentalmente en contar con una base extensiva de usuarios, que publican voluntariamente gran cantidad de información relacionada con su vida cotidiana. El principal problema de esta situación se basa en el hecho de que la información provista por el usuario es, en la mayor parte de los casos, monetizada por parte de la empresa, lo cual puede ser realizado de las más diversas maneras (publicidad personalizada, venta de información personal a terceros interesados, atracción de nuevos usuarios, generación y aprovechamiento de contenido generado por usuarios, entre otros) y ubica

usualmente al individuo, no como un usuario, sino como un producto en la perspectiva de las corporaciones que dirigen tal monetización.

Ante tal perspectiva, la protección de datos se encuentra confrontada con un extraño panorama, en el cual no debe reaccionar ante la amenaza impuesta por entes externos al individuo, sino que se enfrenta con situaciones en las cuales los individuos se ponen en peligro a sí mismos al crear *"sus propios perfiles personales gratuitamente, y voluntariamente revelando mapas detallados de sus relaciones sociales"* (Kartzi, 2008, pág. 9).

Y es que tal como lo afirma Kartzi, desde el punto de vista de la protección de datos las redes sociales representan un peligro siempre presente para el individuo, quien usualmente acepta los términos del servicio sin leerlos (o incluso con el mero hecho de acceder a la página) y se expone "voluntariamente"[123] a riesgos sin precedentes.

La situación originada por las redes sociales se ha visto acrecentada con el surgimiento acelerado de la implementación de tecnologías de telecomunicaciones convergentes. Especialmente por el surgimiento de dispositivos móviles capaces tanto de brindar accesos avanzados a internet al usuario, como de facilitar sus sensores a la plataforma

[123] Entrecomillado puesto que resulta evidente que solamente la corporación propietaria de la red social sabe exactamente lo que se puede lograr con un compendio tan avanzado de información personal constantemente actualizado.
Al respecto, vale la pena recordar que apenas hace pocos meses que fue publicado un estudio en el cual se demostraba cómo, por medio del análisis de los "Likes" brindados por un usuario a los estados de sus amigos o a ciertos bienes o productos en la red social Facebook, es posible determinar con exactitud la personalidad del usuario y clasificarlo dentro de diversos rubros (Kosinski, Stillwell, & Graepel, 2013). Aplicaciones similares para los datos recabados a partir de las redes sociales continuamente salen a la luz, y sin embargo son pocos los usuarios que se enteran de ellas, y muchos menos los que comprenden realmente el peligro que representan.
Finalmente, resulta necesario recordar que el hecho de que la información sea liberada de manera voluntaria no debería significar necesariamente que la misma se encuentre fuera del control del sujeto interesado. Al respecto recomiendo sobremanera la lectura del artículo "Chain-Link Confidentiality" escrito por Woodrow Hartzog (Hartzog, 2012) en la cual el autor propone un sistema de restricciones contractuales interconectadas sobre el uso de la información personal capaz de permitir al individuo rastrear la información personal que libera voluntariamente y ejercer un control activo sobre ella.

social, los cuales agregan y publican gran cantidad de metadatos a la información publicada por el individuo sin su consentimiento informado.

Es necesario resaltar que las redes sociales representan un peligro para sus usuarios en tanto usualmente se encuentran obligadas a facilitar datos personales (o lo hacen voluntariamente con fines de lucro) a entes gubernamentales que procuran agregar tal información a sus ya vastas bases de datos “de seguridad nacional”, cuyos fines y contenidos son completamente secretos, pese a afectar directamente los derechos del interesado.

Tal situación afecta, naturalmente, también intereses de ciudadanos costarricenses, quienes se han insertado a la perfección en las redes sociales más populares. Para septiembre del 2012, tan solo en la red social Facebook se reportaron 1889620 usuarios costarricenses (Miniwatts Marketing Group, 2011), quienes se ven expuestos, al igual que los usuarios del resto del mundo, a los problemas de protección de sus datos personales anteriormente señalados.

Finalmente, puede comprenderse que las redes sociales se ven implicadas también en el problemático abandono de los principios de la protección de datos personales señalados por Rodotà. Especialmente, se relacionan con la problemática de estas plataformas, los principios relativos al tratamiento y a la transmisión de los datos; y fundamentalmente debe hablarse sobre el paulatino abandono del principio de finalidad, el principio de consentimiento, el principio de utilización abusiva y el principio de defensa de los datos especialmente protegidos.

## Traición por Datos de Localización

Desde su introducción en la década de los años 80, las telecomunicaciones móviles han logrado integrarse de maneras insospechadas en nuestra sociedad. Reservadas originalmente a un público exclusivo, las tecnologías móviles son en la actualidad el medio de telecomunicaciones más popular del mundo [124]; actualmente están integradas en los más variados aspectos de nuestra sociedad.

Lastimosamente, la popularización de los dispositivos móviles implicó también el fin de la era en la que toda persona gozaba de verdadera privacidad sobre su ubicación geográfica. El contexto generado por la convergencia tecnológica ha facilitado múltiples afectaciones a la intimidad de los usuarios por el mal uso de sus datos de localización[125], los cuales son recopilados de manera masiva gracias a la unificación de múltiples tecnologías de localización en los dispositivos móviles que utiliza día con día.

En la actualidad es posible determinar la existencia de cuatro tecnologías (Tsai, Gage Kelley, Faith Cranor, & Sadeh, 2010) que trivializan la ubicación geográfica de un usuario, a saber:

- GPS: El sistema de posicionamiento global logra determinar la localización del individuo mediante el rastreo de un dispositivo conectado a una red satelital. Mediante técnicas de triangulación es posible señalar con suma precisión la ubicación exacta del dispositivo.

[124] Tan solo en nuestro país se estima que circulan alrededor de 4404000 teléfonos móviles, lo cual implica que poseemos un nivel de penetración celular superior al 100%

[125] Debe recordarse que en el contexto de las telecomunicaciones móviles adquieren gran relevancia dos conjuntos de datos personales: los datos de tráfico (referidos a la información emitida y recibida por un dispositivo móvil); y los datos de localización (atenientes a la ubicación geográfica del dispositivo).

- Posicionamiento Inalámbrico: La popularidad cada vez mayor de redes inalámbricas en ciudades y campo por igual, abre la posibilidad de realizar un mapeo de los puntos de acceso inalámbrico disponibles por medio de su correlación con direcciones obtenidas por medio de la tecnología GPS.
- Identificación Celular: La tecnología celular actual procura que en todo momento cualquier celular se encuentre conectado a un mínimo de tres antenas, con miras a asegurar el correcto funcionamiento de este. Por medio de técnicas especializadas, tales como la "multilateración"[126], es posible identificar con relativa certeza la localización geográfica de todo dispositivo celular.
- Rastreo de Direcciones IP: Los dispositivos conectados a una red cableada de internet utilizan una dirección IP única que les identifica en la red. El operador de la red conoce tanto la ubicación del abonado donde fue instalada la conexión, como el número de dirección IP asignado al abonado en todo momento.

  En tanto la asignación general de las direcciones IP es de conocimiento público, esto permite identificar en términos generales la ubicación de un dispositivo y, en caso de contar con el apoyo del operador, identificarla exactamente.

Estas cuatro tecnologías pueden ser utilizadas en conjunto por cualquier ente interesado en averiguar la localización exacta de un individuo. Sin embargo, tal como fue establecido a lo largo del punto anterior, en la actualidad esta información es

[126] Técnica que permite triangular la posición geográfica de un aparato móvil conectado a una red celular por medio del cálculo del tiempo que dura su señal en alcanzar las diversas torres celulares cercanas al dispositivo.

comúnmente revelada de manera voluntaria por parte de los individuos, quienes por medio del uso de redes sociales (Facebook, Waze y otros) o de servicios de mensajería instantánea avanzada (Whatsapp, Facebook Messenger, entre otros) constantemente publican (consciente o inconscientemente) su ubicación geográfica.

En este contexto, los datos de localización representan un problema para la protección de datos personales en tanto ellos, al igual que todos los otros tipos de datos, pueden ser agregados entre sí para formar patrones. Tales patrones se encuentran conformados por datos que usualmente no son considerados como sensibles; sin embargo, tal como lo demuestra el estudio *Unique in the Crowd: The privacy bounds of human mobility* (de Montjoye, Hidalgo, Verleysen, & Blondel, 2013), los rastros de movimiento humano son tan únicos que basta con cuatro puntos de localización espacio-temporal para identificar al 95% de los individuos mediante una fórmula matemática[127].

La constante existencia de múltiples fuentes de datos de localización cerca de un individuo ha generado una complicada situación de inseguridad para este, quien pierde día a día su capacidad de determinar con certeza si está siendo rastreado o no (Riofrio, 2013, pág. 1)[128]. Ante tal realidad, resulta evidente considerar la siempre existente amenaza de ser traicionados por nuestros propios datos de localización,

[127] Esta cifra puede dar una idea sobre el verdadero potencial de los datos y metadatos para identificar al individuo que los produce y, por supuesto, de generar fórmulas relacionales que permitan identificar sus patrones de comportamiento tanto en el mundo físico como en el virtual. Finalmente, debemos recordar al lector que el artículo citado no es más que un ejemplo entre miles de potenciales formas de vulnerar la intimidad y la autodeterminación informativa del ciudadano.

[128] Debe recordarse que en la actualidad es común que los marcos normativos aplicables a las tecnologías de telecomunicaciones requieran que todo operador de telecomunicaciones garantice sus servicios y realicen una correcta facturación. Esta exigencia es cumplida por parte de los obligados mediante la retención constante de los datos de localización y tráfico de todo dispositivo conectado a sus redes, los cuales pueden ser puestos a disposición de entes gubernamentales en caso de ser necesario.

como un problema real, por lo que un intento normativo competente debe ser capaz de identificar la vulnerabilidad real relacionada con los datos de localización de un sujeto de datos y proteger de manera amplia tales datos.

En tanto este problema se relaciona con el tratamiento de datos que el usuario usualmente provee sin mayor consideración, o incluso sin saberlo, se puede afirmar que se encuentra relacionado con la teoría de Rodotà, en tanto la tendencia actual de desprotección del sujeto de datos refleja el abandono de los principios de pertinencia, lealtad, información, finalidad, consentimiento, seguridad, responsabilidad y de defensa de los datos especialmente protegidos.

## Transferencias Internacionales de Datos Personales

Podría afirmarse sin temor, que en la actualidad el problema más apremiante en materia de protección de datos personales, se relaciona con la transferencia internacional de datos personales por medio de flujos transfronterizos de datos.

Los flujos transfronterizos de datos son definidos por el centro de las Naciones Unidas sobre corporaciones transnacionales como *"el movimiento a través de límites nacionales de datos computarizados, capaces de ser leídos por una máquina para su procesamiento, almacenamiento o recuperación"* (Centro de las Naciones Unidas sobre Corporaciones Transnacionales, 1982, pág. 8).

Este movimiento de los datos a través de límites nacionales es realizado en la actualidad por medio de las más diversas vías. En este contexto, *"Lo auténticamente*

*determinante en la creación de la globalidad y no solo de los mercados, ha sido la expansión de unas telecomunicaciones transfronterizas, porque en sí mismas no son espaciales, sino metaespaciales. Por no necesitar espacio, no requieren ni siquiera del soporte material de unos cables, basta con el soporte energético de las ondas de diversos tipos"* (Suñé Llinás, 2006, pág. 305).

En los mercados globalizados de la actualidad, prácticamente todo sector de la industria se encuentra inmerso en el manejo de flujos transfronterizos de datos. Estos flujos permiten, entre otros aspectos, la centralización de funciones, la reducción de costos y la integración de servicios (North American Leaders Summit, 2013, pág. 4) y se han constituido actualmente en un verdadero motor del desarrollo y la innovación.

Evidentemente, dentro de los flujos transfronterizos de datos necesarios en un marco global de comercio y comunicaciones electrónicas, puede encontrarse gran cantidad de datos y metadatos relacionados con individuos determinados. Estas transmisiones de datos personales usualmente se encuentran inmersas en un intrincado contexto regulatorio, en el cual los diversos países involucrados procuran proteger, en la medida de lo posible, los intereses individuales, sin limitar innecesariamente los vitales flujos de información.

A pesar de tales esfuerzos, *"Poner límites a este tipo de prácticas es difícil debido al carácter global de La Red y a la interesada anarquía que propicia su nada inocente desregulación, que la somete, más todavía, a la ley de los fuertes. La enorme disparidad de Ordenamientos en materia de Protección de Datos Personales y, sobre todo, los planteamientos tan divergentes, entre la normativa europea y la norteamericana, así como la permisividad que ésta tiene para los intereses empresariales, dificultan hasta el extremo la consecución de unos estándares*

*mínimos razonables, de protección de datos personales en Internet"* (Suñé Llinás, 2006, pág. 320).

Tal como lo establece Suñé Llinás, actualmente es posible observar una serie de situaciones que dificultan la regulación y protección de datos en el contexto creado por los flujos transfronterizos de datos personales. Dada su relación con este tema de estudio, pueden mencionarse como especialmente relevantes las siguientes:

- Irrespeto o incumplimiento internacional de las disposiciones nacionales sobre protección de datos:

  Aquellos intentos por exigir la aplicación de normativa nacional en territorios extranjeros se encuentran usualmente limitados por consideraciones jurisdiccionales. En tanto el Derecho Internacional privilegia especialmente la soberanía estatal en el marco del derecho de autodeterminación de los pueblos, a menos de que se cuente con un tratado internacional que establezca la necesaria aplicación de las disposiciones específicas discutidas, no existirá manera alguna de obligar a otros países a hacer valer la normativa nacional en sus respectivos territorios.

  Esta situación tiene como consecuencia, fundamentalmente, que en el caso de las transferencias internacionales de datos realizadas mediante marcos contractuales fundamentados en jurisdicciones extranjeras, no existirá manera de que un sujeto de datos pueda hacer valer aquellas disposiciones legales de su país que favorezcan sus intereses.

- Liberación sin autorización de los datos una vez que estos han salido del país:

Si bien es cierto que la confianza es fundamento para el comercio (y especialmente para el comercio electrónico), toda transmisión internacional de datos personales implica el peligro de que estos sean liberados, voluntaria o involuntariamente, una vez que se han alejado de la jurisdicción de su país de procedencia.

La siempre presente amenaza de que se presenten este tipo de situaciones, conlleva serios peligros para el sujeto de datos, quien, de no contar con elementos contractuales y económicos suficientes como para reclamar tal liberación ante tribunales arbitrales o legales, será incapaz de hacer valer sus derechos.

- Incapacidad de garantizar el acceso de los sujetos de datos a la información personal en el extranjero:

  Tal como se estudió con anterioridad, parte fundamental de los principios y derechos que rigen los sistemas actuales de protección de datos personales, establecen la necesidad de que todo sujeto de datos sea capaz de acceder a aquella información que le sea relevante, con miras a ejercer de manera eficaz su derecho de autodeterminación informativa.

  En el momento en que los datos salen del territorio nacional, el sujeto de datos puede verse confrontado con su incapacidad de acceder a sus datos personales por motivos de distancia, limitaciones técnicas, o simple y llana mala fe del controlador de los datos.

  Puede encontrarse un buen ejemplo de ello en el internet, en donde una vez que se han ofrecido voluntariamente datos o estos han sido observados o

inferidos por parte de los entes interesados en ellos, resulta prácticamente imposible que como titulares de estos datos, se logre acceder a ellos. Tal situación se da fundamentalmente debido a que una vez liberados nuestros datos en la red, el rastro seguido por ellos se difumina al punto que resulta prácticamente imposible identificar al responsable de su tratamiento.

- Nula o mínima cooperación internacional por los controladores, en la solución de afectaciones o interferencias a la intimidad personal:

  Dado que los controladores extranjeros usualmente no poseen nexo alguno que los atraiga a la jurisdicción nacional, es usual que se nieguen a cooperar con agencias de protección de datos de países externos al suyo.

  Tal situación se torna especialmente tangible en el caso costarricense, en tanto el artículo 45 del reglamento vigente de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, exige a todo controlador de brindar a la Agencia de Protección de Datos (PRODAT) acceso a sus sistemas en calidad de superusuario[129]. En estos términos, serán pocos (si no ninguno) los controladores de datos ubicados en territorios extranjeros que estarán dispuestos a cooperar con nuestra Agencia.

- Dificultades para la investigación de violaciones e imposición de medidas contra infractores ubicados fuera del territorio nacional:

[129] Cuenta especial de usuario utilizada para la administración general del sistema. Brinda privilegios totales sobre el sistema computacional incluyendo la creación, lectura y eliminación de todo tipo de datos, así como la creación de nuevas cuentas de usuarios y la asignación o remoción de privilegios a los usuarios ya existentes. En los sistemas computacionales modernos se considera que la cuenta de superusuario debe ser manejada de manera muy cuidadosa puesto que su uso incorrecto puede acarrear problemas substanciales de seguridad, siendo incluso capaz de causar daños irreparables a este.

En caso de que la agencia de protección de datos del país del sujeto ofendido considere necesario investigar, o que la responsabilidad del controlador haya sido comprobada y que por ello merece la imposición de medidas legales, se verá enfrentada con un complejo panorama legal internacional que usualmente le imposibilita llevar a la práctica tal decisión.

Esta situación se ve empeorada, cada vez que gran cantidad de controladores de datos establecen en sus disposiciones contractuales que el usuario o el sujeto de datos se encontrará vinculado a la jurisdicción más conveniente para el controlador; lo cual tiene como consecuencia la exclusión automática de la agencia de protección de datos de la nación del sujeto de datos y (en aquellos casos en que tales agencias existen en el país del controlador) la inclusión de entes que no consideran obligación suya la proteger los datos de extranjeros.

- Imposibilidad de garantizar la protección de la información personal en aquellos países que no poseen legislación en materia de protección de datos:

  Punto que debería ser evidente considerando las argumentaciones anteriores, en caso de que el país en el cual se encuentre el controlador de datos no posea legislación vinculante en materia de protección de datos personales, el sujeto de datos se encontrará indefenso ante las violaciones a sus intereses.

- Conflicto de leyes o menor protección por las leyes extranjeras que las nacionales:

  Problema de las transferencias internacionales de datos personales que tiene como consecuencia el incremento de la inseguridad jurídica del sujeto de datos, quien no posee verdadero respaldo para confiar en que sus datos

recibirán un nivel adecuado de protección con independencia del lugar al que sean transmitidos.

Se trata de un caso que recuerda la situación de la protección brindada por el marco legal de la Unión Europea, el cual brinda un altísimo nivel de protección a los ciudadanos Europeos. Tal nivel de protección no es alcanzado por la mayor parte de los países del orbe, por lo que la Unión Europea se ha visto en la obligación de establecer límites a las transferencias internacionales de datos personales.

- Acceso y tratamiento no autorizado a la información por parte de gobiernos extranjeros:

  Problema especialmente controvertido, dado que comúnmente se justifica tal acceso gubernamental en razones de seguridad nacional (límite al derecho de autodeterminación informativa).

  Este es el caso del gobierno estadounidense, el cual afirma con base en su Patriot Act, su potestad de acceder a toda información procesada, transmitida o almacenada dentro de su jurisdicción, independientemente de la nacionalidad del sujeto de datos. Esta situación ha causado gran revuelo dada la gran cantidad de información que es enrutada a través de infraestructura estadounidense[130].

[130] Al respecto se recomienda la lectura de la siguiente fuente: http://blogs.computerworlduk.com/cloud-vision/2012/05/us-patriot-act---can-uk-cloud-customers-use-us-cloud-providers/index.htm que analiza la potestad real de que la jurisdicción estadounidense pueda ser extendida de esta manera.

- Decisiones jurisdiccionales externas al país del sujeto de datos que requieran la liberación para fines comerciales o la prestación de la información personal que se encuentre dentro de su jurisdicción:

  En intensa relación con el punto anterior, dados los conflictos jurisdiccionales existentes y la disparidad en la protección brindada a los datos personales por los diversos sistemas legales, las transferencias internacionales de datos personales pueden dar pie a violaciones a los intereses de los sujetos de datos, por verse el controlador obligado, por orden judicial, a liberar los datos para diversos fines no autorizados por el interesado.

- Problemas relacionados con la recuperación, manejo y destrucción de la información personal:

  En tanto el controlador de los datos se encuentra fuera de la jurisdicción nacional, resulta prácticamente imposible asegurar que este cumpla con los principios y disposiciones legales aplicables al tratamiento de datos personales. Tal situación se torna especialmente relevante en tanto no existe manera alguna (salvo disposiciones contractuales que por lo general son excepcionales) de asegurar al sujeto de datos que estos no incluyen información sensible, o que esta no se encuentra en riesgo de ser liberada, por no cumplir el controlador con los principios de seguridad de la información pertinentes.

- Problemas relacionados con la aplicación del derecho al olvido:

  Evidentemente, las dificultades ya señaladas causadas por las transferencias internacionales de datos personales implican que el sujeto no posee manera de ejercer control directo sobre sus datos, ni cuenta con apoyo efectivo por parte

de las instituciones gubernamentales creadas para tal fin. Esta situación tiene como consecuencia que en la práctica el individuo no posee medios directos de solicitar la completa eliminación de sus datos, ni puede estar seguro de que estos serán eliminados automáticamente pasado un lapso prudencial de tiempo (ambos aspectos fundamentales del derecho al olvido).

- Pérdida de confianza por parte de los sujetos de datos por las afectaciones sufridas:

  En tanto los peligros representados por la transferencia internacional de datos afectan tanto al sector privado como al sector público, toda afectación o violación a los intereses del sujeto de datos que sea realizada en el marco de tales transferencias, exponen a las instituciones involucradas a pérdidas en su credibilidad y en la confianza que los sujetos han depositado en ellas.

  Tal situación se torna especialmente preocupante en el marco nacional, en tanto en los últimos tiempos se ha podido observar cómo el gobierno ha impulsado la utilización de tecnologías descentralizadas con miras a minimizar el gasto público en infraestructura. Especialmente relevante resulta la Directriz Nº 46-H-MICITT del 9 de abril del 2013 que insta al sector público a la adquisición de "*soluciones de cómputo en la nube sobre otro tipo de infraestructura. Esto aplica para equipos, licencias y sistemas informáticos, servidores de hospedaje de páginas Web, servidores de aplicaciones, correo electrónico, muros de fuego, sistemas operativos, sistemas ofimáticos, bases de datos u otras tecnologías informáticas ya sea para el usuario final o para el centro de datos en sí, o cualquier otro tipo de desarrollo tecnológico"* (Poder Ejecutivo de la República de Costa Rica, 2013), las cuales

generalmente requieren de la realización de transferencias internacionales de datos personal para su correcto funcionamiento.

Debe concluirse aceptando que en la actualidad las transferencias internacionales de datos personales representan un punto álgido de la regulación vigente en materia de protección de datos, dado el carácter sensible del objeto de las transferencias y la íntima relación de estos con los bienes y servicios que día con día se consideran más necesarios para nuestras vidas.

Las transmisiones internacionales de datos personales afectan a individuos del mundo entero, independientemente de su nacionalidad, y al igual que en otros casos ya estudiados, es posible identificar situaciones en que estas han producido afectaciones directas a intereses costarricenses.

Específicamente, es necesario recordar en este punto la situación ocurrida en el año 2002, en la cual salió a la luz pública la existencia de un contrato privado por un valor de once millones de dólares entre la empresa ChoicePoint Inc. y el gobierno estadounidense, en los cuales la empresa ofrecía la venta de datos (nombre, cédula, género, fecha de vencimiento de pasaporte y otros) de ciudadanos costarricenses a un precio de 30 dólares, por búsqueda individual (EPIC.org, 2002). Los datos en cuestión eran transmitidos, sin autorización de los interesados, a los servidores de la empresa ubicados en el extranjero y posteriormente eran puestos a disposición del gobierno en cuestión.

La venta de datos personales al gobierno estadounidense dio a lugar a uno de los mayores escándalos que, en materia de protección de datos personales, ha visto el

país (Ver Anexo 9), lo cual dio impulso a uno de los muchos proyectos dirigidos a la creación de legislación costarricense en materia de protección de datos personales[131] (Departamento de Estado de los Estados Unidos de América, 2003, pág. 12).

Tomando en consideración que nuestro país posee ya un historial de afectaciones a los intereses de sus sujetos de datos, puede concluirse que una adecuada propuesta legislativa debe abarcar oportunamente la problemática de las transferencias internacionales de datos personales y procurar una solución holística a ella.

Finalmente, debe reconocerse que los flujos transfronterizos de datos implican usualmente tanto el tratamiento como la transmisión de los datos personales, por lo que una caracterización de los principios afectados por estos debe admitir que la manera en que ha sido abordado este tema, conlleva el abandono de todos los principios relacionados con estas dos etapas.

### Violaciones a la Autodeterminación Informativa por otros Estados

Tal como se estudiara con anterioridad, uno de los límites principales al derecho de autodeterminación informativa se encuentra en las excepciones que pueden ser creadas por las medidas tomadas legítimamente, dirigidas a salvaguardar la "seguridad nacional", concepto que hace referencia a la noción de relativa estabilidad, calma o predictibilidad que se supone beneficiosa para el desarrollo de un país.

[131] En este punto debe resaltarse que a pesar de lo conocida que fue la situación, las múltiples promesas políticas realizadas no llevaron a cambios reales en la situación del país, no siendo aprobada la ley prometida sino hasta el 5 de septiembre de 2011. Asimismo, se debe resaltar que para este momento la situación de venta de datos personales en el país había tomado una dirección preocupante, especialmente con la compra en el año 2010 de la empresa de información crediticia Datum S.A. por la empresa estadounidense Equifax, a la cual pertenece ChoicePoint Inc. (Rhodes, 2013).

Si bien clásicamente la seguridad nacional hacía referencia fundamentalmente a la protección del país frente a amenazas militares foráneas, a partir de los eventos sucedidos el 11 de septiembre del 2001, da inicio un proceso global de ampliación de los objetivos de la seguridad nacional, en el cual se brinda especial importancia a las amenazas difusas que plantean los actos terroristas, la criminalidad digital y los fenómenos sociales de gran escala (disturbios populares, inmigraciones masivas, entre otros).

Según Alcántara, este proceso de ampliación de los objetivos de la seguridad nacional responde al fenómeno conocido como la política del miedo, en la cual *"se presentan al pueblo una serie de amenazas difusas y caóticas (como el "terrorismo internacional") como excusa para conseguir que se acepten políticas de recorte de derechos y de vigilancia masiva de la ciudadanía (como el derecho al secreto de las comunicaciones, el derecho a la intimidad o la aceptación de tratos indignos en controles aeroportuarios) a cambio de ayudar a preservar el orden y la fuerza del Estado que apresa y encarcela a los terroristas, manteniendo así ese caos profetizado en un segundo plano de la realidad"* (Alcántara, 2008, pág. 79).

Tal como lo asegura el autor, desde el punto de vista de los derechos humanos, la política del miedo tiene como consecuencia un verdadero cambio de paradigma. La validación de amplias excepciones a los derechos individuales y la necesidad de oponerse a aquel enemigo invisible mediante la implementación de medidas de seguridad y vigilancia, culminan con a la aceptación de la seguridad nacional como un asunto que legitima al Estado en sus esfuerzos por lograr el íntegro control y rastreo de todo aquello que suceda dentro (y fuera) del territorio nacional.

Para lograr tan necesario control, los gobiernos han encontrado en las tecnologías de la información y la comunicación un poderoso aliado. Por medio de técnicas como la video vigilancia, la retención de datos de telecomunicaciones, el rastreo satelital y la adquisición de datos biométricos de sus ciudadanos, las agencias de inteligencia han sido capaces, a lo largo de la última década, de adquirir grandes cantidades de información con miras a la detección de amenazas potenciales[132].

Para los usuarios, el panorama pintado por esta conjunción entre la imperativa vigilancia, las excepciones a sus derechos humanos y la alta tecnología, no ha sido nada halagüeño. A lo largo de la década pasada, el número de potenciales afectaciones a los derechos fundamentales ha aumentado extraordinariamente, y si bien es cierto que en la actualidad los peligros difusos a la seguridad nacional son evidentes, también se han hecho evidentes los peligros y quebrantos a la intimidad y autodeterminación informativa de los individuos, causados por los mismos sistemas que buscan protegerlos.

En la implementación de las ideas de la política del miedo, es creado, en el nombre de la seguridad nacional, un *"panóptico estatal omnipresente y coercitivo; un sistema perfectamente vigilado donde todo es, en todo momento, controlado por los vigilantes"* (Alcántara, 2008, pág. 96) en el que los principios democráticos son dejados de lado y (entre muchos, muchos otros) el derecho de autodeterminación informativa deja de ser relevante frente a los intereses y poderes estatales.

[132] El auge de las cámaras de seguridad, la creación de vehículos autónomos de monitoreo aéreo (drones), y la implementación de sistemas de identificación biométrica a distancia, son todos ejemplos de su creciente capacidad de análisis y recolección de datos con el fin último de identificar amenazas potenciales.

La década del 2000 vio el inicio del tránsito desde la sociedad democrática hacia la sociedad del control, una sociedad totalitaria en la que los difusos intereses del pequeño grupo de personas que marcan el rumbo de las políticas mundiales privan sobre los del resto. En esta nueva sociedad, el Estado ha encontrado en la "seguridad nacional" una llave maestra capaz de eliminar toda restricción a su capacidad de acceder, tratar y almacenar de manera masiva la información personal de cualquier individuo.

Con base en esta imperativa necesidad de contar con acceso a aquella información necesaria para la defensa de la seguridad nacional, a lo largo de la década del 2000 fue posible apreciar un tránsito desde una concepción de respeto a los principios fundamentales de la autodeterminación informativa, hacia la creación de nuevos principios, dirigidos esta vez no a la protección del ciudadano, sino a la facilitación de las transferencias de información con independencia de la voluntad del sujeto de datos[133].

Las consecuencias que tal fenómeno ha tenido para la protección de datos personales bien ha sido identificada por Rodotà, quien afirma que: *"Esta recogida de datos personales a escala de masa ya ha determinado la transformación de todos los ciudadanos en potenciales sospechosos, frente a los poderes públicos, y la objetivación de la persona, frente al sistema de las empresas. Además, la creciente posibilidad por parte de sujetos públicos de interconectar todos sus bancos de datos y de obtener información de cualquier fuente privada produce una transparencia social sin precedentes, que cambia la posición del ciudadano en las sociedades democráticas y su relación con el Estado"* (Rodotà, 2006, pág. 57).

[133] Ejemplo de dichos principios se encuentra en el ya mencionado "principio de disponibilidad", el cual "Establece básicamente que la información de que disponen los países miembros debe intercambiarse con la mayor celeridad posible entre los servicios policiales" (Dietrich Plaza, 2007, pág. 39).

Las palabras de Rodotà parecieran actualmente poseer un carácter profético. Gracias a denuncias[134] como las realizadas por Edward Snowden, poco a poco han salido a la luz pública las incontables[135] violaciones a la autodeterminación informativa, al secreto de las comunicaciones y a los principios de la protección de datos personales realizadas por parte de gobiernos del mundo.

Así, el año 2013 (y los inicios del 2014) se han caracterizado por una explosión de información que ha puesto en evidencia los diversos proyectos secretos implementados diversos gobiernos, con miras a realizar un espionaje profundo de los datos e informaciones transmitidas por los ciudadanos del mundo. Esta situación posee el potencial para afectar seriamente los derechos e intereses de todo individuo, quien pasará de ser percibido por su Estado como un ciudadano y soberano de un país en democracia, a ser simplemente otro sujeto, a ser controlado y vigilado en una realidad que cada vez se asemeja más a las distopías sobre las que nos advertían ya Orwell y Bentham.

[134] Sobre el tema se recomienda ver (Greenwald & MacAskill, NSA Prism program taps in to user data of Apple, Google and others, 2013), (Shane & Somaiya, 2013) y (Greenwald, MacAskill, & Poitras, 2013) entre otros.
[135] Ver (Ackerman, 2013).

### *Síntesis de la Segunda Sección*

Fundamentos de Telecomunicaciones

*A lo largo de la cual se examina la historia y los fundamentos técnicos que soportan la convergencia de las telecomunicaciones, para a continuación adentrarse en el estudio de los efectos que esta ha tenido en el plano regulatorio nacional e internacional.*

- *"La comunicación consiste en la transferencia de información en varias formas (texto, audio, video) de un lugar a otro. Este proceso requiere por lo menos tres elementos: una fuente de información, un medio que transporte dicha información a un punto remoto y un elemento dedicado a recuperar la información transmitida" (Przemyslaw & Slawomir, 2009).*
- A lo largo de la historia, los seres humanos han ideado y utilizado diversos sistemas de comunicación. Puede afirmarse que la historia de las telecomunicaciones modernas da inicio en el siglo XIX y se desarrolla especialmente a lo largo del siglo XX con la creación de redes nacionales de telecomunicaciones, la creación de los primeros entes internacionales dirigidos a la coordinación de estos sistemas y la posterior apertura de los mercados.
- La rápida evolución de las TICs a lo largo del siglo XX conlleva también una serie de importantes cambios económicos, industriales, y regulatorios que configuran la convergencia de las telecomunicaciones. Actualmente esta convergencia se nos presenta como una realidad innegable que, según Aldana & Vallejo, surgen a partir de tres olas tecnológicas, a saber:
    - Primera ola: de las telecomunicaciones analógicas a las telecomunicaciones digitales. Relacionada, tal como lo establece su nombre, con el abandono progresivo de tecnologías analógicas en favor de sus contrapartes digitales. Según las autoras, este proceso solamente fue posible gracias a los siguientes desarrollos tecnológicos:
        - Digitalización de redes: la cual viene a significar el surgimiento de nuevas oportunidades y servicios innovadores aunados con un menor costo de operación y un incremento en la efectividad de la red. Asimismo, este cambio conlleva grandes implicaciones desde el punto de vista regulatorio, pues disminuye la carga

sobre el espectro radioeléctrico y posibilita la prestación de múltiples servicios por un solo medio.

- Desarrollo de la informática: el cual no solamente posibilita el procesamiento de las gigantescas cantidades de información producida por las redes digitales y la popularización de dispositivos de acceso a las redes; sino que también demuestra mediante sus avances constantes la necesidad imperiosa de aumentar la eficiencia de las redes y las grandes ganancias que dicho esfuerzo conllevaría para todos los interesados.
- Conmutación de paquetes: desarrollo tecnológico que brinda soluciones a uno de los problemas originales de las redes de telecomunicaciones modernas: la centralización, ineficiencia y vulnerabilidad de la infraestructura de telecomunicaciones analógicas.

- Segunda ola: el surgimiento de las *redes de nueva generación*: La cual aprovecha fundamentalmente los cambios tecnológicos derivados de la primera ola para generar los primeros ejemplos de convergencia tecnológica y aplicarlos de manera cada vez mayor en el sector telecomunicaciones; esto conlleva también modificaciones importantes en la organización de los mercados, el uso dado a las tecnologías por parte de los usuarios, y la manera en que estas nuevas situaciones son reguladas en los ámbitos nacional e internacional.
- Tercera ola: nuevas aplicaciones de las TICs: Caracterizada fundamentalmente por la innovación y la convergencia tecnológica, esta tercera ola tiene lugar tanto en el pasado cercano como en la actualidad. Es un proceso incompleto basado en la generación de nuevas opciones tecnológicas, organizacionales y regulatorias con miras a maximizar los beneficios de las TICs.

- Estas tres olas tecnológicas tienen como consecuencia que en la actualidad nos encontremos inmersos en la llamada convergencia de las telecomunicaciones, proceso que tal como se ha estudiado no se limita a la mera capacidad de

brindar múltiples servicios por un único medio de comunicación, sino que unifica dentro de sí una serie de cambios estructurales que demarcan la manera en que el sector telecomunicaciones opera y su relación con los usuarios finales.

- En palabras de Aldana & Vallejo, *"La convergencia pone a prueba los modelos de negocios tradicionales, genera competencia entre plataformas independientes y ejerce presión sobre los operadores tradicionales, cambia la conducta del consumidor y lo hace más activo en la demanda de servicios, y lleva a que los procesos de gestión de tecnología sean dinámicos. A su vez, estos cambios tecnológicos y de mercado ejercen presiones sobre los organismos de regulación para que se adapten al nuevo entorno (Aldana J. & Vallejo C., 2010, pág. 173)"*.
- La convergencia de las telecomunicaciones ha tenido efectos directos en los fenómenos sociales, económicos, políticos y tecnológicos que conforman gran parte de nuestra realidad. Estos efectos se han visto traducidos tanto en el nivel nacional como el internacional en la evolución normativa y de los marcos regulatorios.
- En el plano regulatorio nacional, las principales consecuencias de la convergencia de las telecomunicaciones se relacionan tanto con el reconocimiento legal de las nuevas materias y temas relevantes a los cambios tecnológicos, como con la adopción de modelos de desarrollo compatibles con los nuevos mercados de telecomunicaciones; esto asigna nuevos roles al Estado.
- En el ámbito internacional, la convergencia de las telecomunicaciones ha tenido como fundamental consecuencia la creación de una serie de instituciones que realizan sus labores de dirección y regulación, por medio de un modelo de gobernanza innovador (modelo de múltiples interesados) contrapuesto en muchos sentidos con el modelo tradicional (de gobernanza multilateral) que caracteriza las labores de entes como la Unión Internacional de las Telecomunicaciones.
    - La Unión Internacional de las Telecomunicaciones y el Modelo de Gobernanza Multilateral: encargada históricamente de la regularización y estandarización internacional de las telecomunicaciones tradicionales,

esta agencia especializada de la ONU basa su modelo de gobernanza en un sistema de diálogo multilateral que procura brindar igual voz y voto a los países miembros.

- La Gobernanza de Internet y el Modelo de Múltiples Interesados: Uno de los máximos ejemplos de la convergencia de las telecomunicaciones, el internet, presenta un especial reto para todo esfuerzo regulatorio en tanto es una red intangible, fundamentalmente extraterritorial, sobre el cual ningún país, individuo o corporación puede alegar titularidad exclusiva; por lo cual plantea problemas globales que requieren de soluciones globales.

  En este contexto, el modelo de gobernanza por múltiples interesados, propone asegurar la participación activa de todos los actores potencialmente interesados en la toma de decisiones, por medio de un proceso "de abajo hacia arriba" basado en el consenso y no en la imposición.

## Problemas Emergentes de la Protección de Datos Frente a la Convergencia de las Telecomunicaciones

*A lo largo de la cual se examina de manera detenida cinco de los mayores problemas que afectan a la protección de datos personales en el contexto creado por las comunicaciones convergentes.*

- Actualmente la protección de datos personales se enfrenta a un amplio grupo de problemas emergentes que, según Stefano Rodotà, pueden deberse a tres razones fundamentales:
  - la reducción de garantías y el cambio de los criterios de referencia a partir de los hechos ocurridos el 11 de septiembre de 2001;
  - la extensión de esta tendencia de reducción de garantías a sectores no relacionados que intentan sacar ventajas de la mutación del clima general;

  - los continuos y crecientes instrumentos de clasificación, selección y control de las personas, ofrecidos por las nuevas tecnologías que determinan una situación de deriva tecnológica, ante las cuales ni las autoridades nacionales ni las internacionales logran responder adecuadamente.

- Esta cadena de acontecimientos no solamente ha producido una erosión de los principios del sistema de protección de datos, sino que también ha definido un nuevo conjunto de tendencias dirigidas hacia la totalidad, la permanencia y la disponibilidad de las informaciones recogidas.
- En el contexto actual es posible encontrar múltiples áreas de la protección de datos personales que se han visto afectadas por este proceso de degradación. Algunos de los problemas emergentes más relevantes encontrados son:
  - Proliferación de Cookies
    - El aumento en la prevalencia de mecanismos dirigidos al rastreo sin consentimiento del comportamiento individual por medio de internet, vulneran de manera importante los derechos humanos.
    - El uso indiscriminado de cookies en los sistemas informáticos aunado con la inconsciencia entre los usuarios sobre la situación, ha sido aludida por los diversos sistemas legales de maneras muy diversas, a pesar de lo cual no ha sido posible encontrar una respuesta definitiva al problema.
    - Frente a esta situación, la tesis del abandono de los principios de la protección de datos sostenida por Rodotà adquiere gran relevancia, en tanto resulta imposible afirmar que sean realmente aplicados los principios de pertinencia, lealtad, información, licitud y defensa de los datos en un contexto caracterizado por su secretismo para con el usuario y dedicado abiertamente al uso comercial de los datos recabados.
  - Elaboración de Perfiles y Redes Sociales
    - El surgimiento de las redes sociales ha implicado un cambio completo en el paradigma de los sistemas de protección de

datos personales al involucrar activamente al sujeto de datos en el proceso de recopilación de la información y de generación de perfiles sociales.

- *"En el contexto de las redes sociales, los usuarios eligen divulgar información personal con miras a "hacer un perfil" de sí mismos y para participar en la comunidad de usuarios. Ellos publican una "identidad personal" al publicar selectivamente información personal en sus perfiles. Esta identidad digital es su representación en el mundo en línea y para algunos usuarios una "manifestación de (…) personalidad," La conexión entre la persona en línea y la realidad fuera de línea del individuo es, usualmente, un aspecto importante de la mayor parte de las redes sociales. Esto es obvio especialmente cuando los usuarios participan con sus nombres verdaderos y publican fotografías de sí mismos. El sentido de "encontrarse conectado", usualmente con una comunidad fuera de línea o con una nueva comunidad en línea, creada por una red social, es parte de su éxito y parte del reto desde la perspectiva de la privacidad" (Kartzi, 2008, pág. 7).*
- El surgimiento de las redes sociales aparejó, dentro de sus miles de consecuencias, problemas relacionados con la monetización, contextualización, centralización y deshumanización del ser humano; el cual deja de ser percibido como un usuario y pasa a ser el verdadero producto que da valor a dichas redes.
- Esta situación apareja grandes consecuencias de las cuales no escapan los usuarios costarricenses (para 2012 tan solo en Facebook se reportaban casi dos millones de usuarios de nuestro país).
- Nos encontramos en este caso ante la vulneración de todos aquellos principios relacionados con el tratamiento y la transmisión de los datos y, especialmente, de los principios de finalidad, consentimiento, (no) utilización abusiva y el principio de defensa de los datos especialmente protegidos.

- Traición por Datos de Localización
  - La popularización actual de los dispositivos móviles implicó también el fin de la era en la que toda persona gozaba de verdadera privacidad sobre su ubicación geográfica. El contexto generado por la convergencia tecnológica, ha facilitado la afectación a la intimidad de los usuarios por el mal uso de sus datos de localización, los cuales son recopilados de manera masiva gracias a la unificación de múltiples tecnologías de localización, en los dispositivos móviles que utilizan día con día.
  - En este contexto, los datos de localización representan un problema para la protección de datos personales en tanto ellos, al igual que todos los otros tipos de datos, pueden ser agregados entre sí para formar patrones. Tales patrones se encuentran conformados por datos que usualmente no son considerados datos sensibles; sin embargo, tal como lo demuestra el estudio Unique in the Crowd: The privacy bounds of human mobility (de Montjoye, Hidalgo, Verleysen, & Blondel, 2013), los rastros de movimiento humano son tan únicos que basta con cuatro puntos de localización espacio-temporal para identificar al 95% de los individuos mediante una fórmula matemática.
  - Esta situación ha degenerado en la actualidad en la pérdida de la capacidad del individuo de saber si está siendo rastreado o no (Riofrio, 2013, pág. 1); lo cual pone en evidencia el actual abandono de los principios de pertinencia, lealtad, información, finalidad, consentimiento, seguridad, responsabilidad y de defensa de los datos especialmente protegidos.
- Transferencias Internacionales de Datos Personales
  - Los flujos transfronterizos de datos son definidos por el centro de las Naciones Unidas sobre corporaciones transnacionales como *"el movimiento a través de límites nacionales de datos computarizados, capaces de ser leídos por una máquina para su*

*procesamiento, almacenamiento o recuperación" (Centro de las Naciones Unidas sobre Corporaciones Transnacionales, 1982, pág. 8).*

- En la actualidad los flujos transfronterizos de datos incluyen una cantidad increíble de datos personales, los cuales presentan una serie de dificultades a todo esfuerzo regulatorio, dentro de los que se encuentran las siguientes:
    - Incumplimiento, en el ámbito internacional, de las disposiciones nacionales sobre protección de datos.
    - Liberación sin autorización de los datos una vez que estos han salido del país.
    - Inhabilidad de garantizar el acceso de los sujetos de datos a la información personal en el extranjero.
    - Inhabilidad o falta de voluntad en la cooperación internacional.
    - Dificultades para la investigación de violaciones e imposición de medidas contra infractores ubicados fuera del territorio nacional.
    - Imposibilidad de garantizar la protección de la información personal en aquellos países que no poseen legislación sobre la materia.
    - Conflicto de leyes o menor protección por las leyes extranjeras que las nacionales.
    - Acceso y tratamiento no autorizado a la información por parte de gobiernos extranjeros.
    - Decisiones jurisdiccionales externas que requieran la liberación o prestación de la información que se encuentre dentro de su jurisdicción.
    - Problemas relacionados con la recuperación, manejo y destrucción de la información personal.
    - Problemas relacionados con la aplicación del derecho al olvido.

- Pérdida de confianza por parte de los sujetos de datos en el gobierno de su país frente a potenciales afectaciones a su información.

- Debe reconocerse que los flujos transfronterizos de datos implican usualmente tanto el tratamiento como la transmisión de los datos personales, por lo que una caracterización de los principios afectados por estos, debe admitir que la manera en que ha sido abordado este tema conlleva el abandono de todos los principios relacionados con estas dos etapas.

- Violaciones a la Autodeterminación Informativa por Parte de Gobiernos
  - Uno de los límites principales al derecho de autodeterminación informativa se encuentra en las excepciones que pueden ser creadas por las medidas tomadas legítimamente dirigidas a salvaguardar la "seguridad nacional", concepto que hace referencia a la noción de relativa estabilidad, calma o predictibilidad que se supone beneficiosa para el desarrollo de un país.
  - A partir del 11 de septiembre de 2001 da inicio un proceso global de ampliación de los objetivos de la seguridad nacional, que se enfoca en las llamadas "amenazas difusas" como parte de un conjunto de "políticas del miedo" (Alcántara, 2008, pág. 79), que tiene como consecuencia un cambio de paradigma y la validación de amplias excepciones a los derechos individuales.
  - Para lograr tan necesario control, los gobiernos han encontrado en las tecnologías de la información y la comunicación un poderoso aliado. Por medio de técnicas como la video vigilancia, la retención de datos de telecomunicaciones, el rastreo satelital y la adquisición de datos biométricos de sus ciudadanos, las agencias de inteligencia han sido capaces, a lo largo de la última década, de adquirir grandes cantidades de información con miras a la detección de amenazas potenciales.

- Las consecuencias que tal fenómeno ha tenido para la protección de datos personales bien ha sido identificada por Rodotà, quien afirma que: *"Esta recogida de datos personales a escala de masa ya ha determinado la transformación de todos los ciudadanos en potenciales sospechosos, frente a los poderes públicos, y la objetivación de la persona, frente al sistema de las empresas. Además, la creciente posibilidad por parte de sujetos públicos de interconectar todos sus bancos de datos y de obtener información de cualquier fuente privada produce una transparencia social sin precedentes, que cambia la posición del ciudadano en las sociedades democráticas y su relación con el Estado" (Rodotà, 2006, pág. 57).*

# Título Segundo: La Protección de Datos en el Ámbito Internacional. Funcionamiento y Normativa Relevante para las Telecomunicaciones Convergentes

## Capítulo I: Marcos Legales Representativos en Materia de Protección de Datos en el Derecho Comparado

El presente capítulo procurará examinar algunos de los marcos legales de protección de datos más representativos que existen actualmente en el mundo y que son aplicados tanto regional como nacionalmente. Específicamente se enfocará el estudio de cuatro sistemas legales, a saber: El modelo europeo de protección de datos (que puede considerarse de regulación máxima), el sistema estadounidense de regulación mínima o autorregulación, el sistema de protección constitucional (o habeas data) adoptado por gran parte de los países latinoamericanos, y algunos de los sistemas que han optado por proteger los datos personales solamente por la vía legal.

## Sección I: Modelo Europeo y Sistema Norteamericano

A lo largo de esta primera sección se estudiarán dos sistemas legales que tradicionalmente han sido considerados como diametralmente opuestos entre sí. Se trata, por supuesto del Marco Europeo de Protección de Datos y a las políticas que sobre el tema han sido aplicadas por el sistema norteamericano.

A lo largo de dicho estudio se hará énfasis en dilucidar las características intrínsecas de dichos sistemas y el marco normativo que los fundamenta. Así, en el caso del sistema Europeo, se iniciará el estudio mencionando algunas de las características más representativas de dicho sistema, para a continuación enfocarse en los diversos tratados internacionales que lo fundamentan, y finalmente adentrarse en el examen de las diversas directivas, regulaciones y reformas que lo constituyen.

Una vez completado el estudio del sistema europeo, se procede a examinar detenidamente el marco legal federal norteamericano. Dentro de este, se centrará la atención en las más de treinta leyes federales que se relacionan con la el derecho a la privacidad y a la protección de datos personales y se culminará con la mención de un novedoso proyecto que busca regular por vez primera, el tema de si en sector privado pueden darse los datos personales.

### *Marco Europeo de Protección de Datos Personales*

Caracterizado por los altos estándares que regulan la materia de la protección de datos personales, el Marco Europeo de Protección de Datos se constituye actualmente como el referente obligatorio de todo esfuerzo por regular la materia, en tanto constituye el único ejemplo verdaderamente funcional de un sistema internacional de protección de datos.

Tal como se estudió con anterioridad, Europa no solamente es la cuna de la protección de datos moderna, sino que posee en la actualidad el sistema más complejo (y completo) de protección de datos en el ámbito mundial. La Unión Europea es una región donde *"múltiples sistemas legales son aplicables actualmente a la privacidad y a la protección de datos en diversos contextos, sea en el contexto del derecho privado internacional y entre entidades comerciales, o en el contexto del uso de los datos personales en las labores policiales y de investigación judicial"* (Linskey, Robinson, & Greenberg, 2010, pág. 4).

Efectivamente, fundamentado directamente en las declaraciones internacionales de derechos humanos y los tratados constitutivos de la Unión Europea, este sistema procura lograr la protección de los datos personales a partir del establecimiento e implementación de una serie de *directivas y regulaciones* que no solo dirigen los esfuerzos de todos los países miembros, sino que también establecen estándares y principios mínimos de protección aplicables entre ellos.

Con miras a estudiar las complejidades intrínsecas del Marco Europeo de Protección de Datos Personales y con miras a brindar al lector una mejor comprensión de las maneras en las que sus diversos elementos se relacionan entre sí, a continuación se

realizará un examen detallado de la principal normativa relevante[136], comenzando por las declaraciones y tratados internacionales que lo fundamentan, pasando por las diversas directivas y regulaciones relacionadas con el tema y concluyendo con una explicación de las reformas planteadas a dicho sistema que serán pronto llevadas a la práctica.

## Marco Legal Fundamental

### *Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01)*

Declarada solemnemente el 7 de diciembre del 2000, la carta de Derechos Fundamentales de la Unión Europea consagra una serie de derechos políticos, sociales y económicos para los ciudadanos y residentes de la Unión, dentro del marco legislativo europeo. Si bien sus efectos no se dieron sino hasta la entrada en vigencia del tratado de Lisboa en el año 2009, se trata de un paso fundamental hacia la unificación normativa de los países miembros.

La carta posee carácter vinculante para toda corte que aplique el marco normativo europeo, y posee la particularidad de considerar, a lo largo de su artículo 8, a la protección de datos personales como un derecho fundamental, según el cual toda persona puede exigir que todo tratamiento de sus datos sean realizados *"de modo leal,*

[136] Por motivos de espacio no se podrá abarcar en este punto la gran cantidad de jurisprudencia relevante al tema, sin embargo, para un estudio detallado de esta se recomienda revisar las fuentes oficiales de la Unión Europea, y especialmente la página web que ha dedicado la Comisión Europea al estudio de la legislación y la jurisprudencia relevante - ver (Comisión Europea, 2013).

*para fines concretos y sobre la base del consentimiento de la persona afectada"*. Más aún, reconoce dicho artículo el *"derecho de toda persona a acceder a los datos recogidos que la conciernan y a su rectificación"*, siendo el respeto de las normas atenientes a la protección de los datos personales *"sujeto al control de una autoridad independiente" (Parlamento Europeo, Consejo de la Unión Europea y Comisión Europea, 2000).*

Dicho artículo *"se encuentra inspirado, y es basado en, una variedad de instrumentos legales a pesar de que la protección de datos personales no es reconocida como un derecho específico en el marco existente de instrumentos internacionales dirigidos a la protección de los derechos humanos. Inicialmente, es derivado del artículo 8 de la Convención Europea de Derechos Humanos, incluyendo la jurisprudencia de la Corte Europea de Derechos Humanos, sobre la protección de la privacidad y la vida privada, a pesar de que la protección de los datos personales no se encuentra explícitamente mencionada en la Convención como tal"* (EU network of independent experts on fundamental rights, 2006, pág. 90).

### *Tratado de la Unión Europea*

Firmado el 7 de febrero de 1992, el Tratado de la Unión Europea constituye el pilar fundamental que dirige el funcionamiento de la Unión. A lo largo de este texto normativo se establecen las bases institucionales que rigen el modelo internacional aplicado en Europa, a la vez que reconoce fundamentos y principios de Derecho aplicables para dicho modelo[137].

[137]Específicamente los principios de atribución, subsidiariedad y de proporcionalidad, los cuales, de conformidad con el artículo 5 de dicho tratado, delimitan las competencias de la Unión con respecto a los Estados miembros.

En el contexto de la protección de datos personales, el tratado adquiere importancia al establecer disposiciones relevantes a lo largo de sus artículos 6 y 39, las cuales dictan lo siguiente:

"Artículo 6

*1. La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados.*

*Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados.*

*Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones.*

*2. La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta adhesión no modificará las competencias de la Unión que se definen en los Tratados.*

*3. Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales" (Unión Europea, 2008).*

*"Artículo 36*

*El Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad consultará periódicamente al Parlamento Europeo sobre los aspectos principales y las opciones fundamentales de la política exterior y de seguridad común y de la política común de seguridad y defensa y le informará de la evolución de dichas políticas. Velará por que se tengan debidamente en cuenta las opiniones del Parlamento Europeo. Los representantes especiales podrán estar asociados a la información al Parlamento Europeo" (Unión Europea, 2008).*

*El Parlamento Europeo podrá dirigir preguntas o formular recomendaciones al Consejo y al Alto Representante. Dos veces al año procederá a un debate sobre los progresos realizados en el desarrollo de la política exterior y de seguridad común, incluida la política común de seguridad y defensa.*

Tal como puede comprender el lector, los artículos anteriormente mencionados fundamentan la protección de datos a lo largo de Europa al establecer parámetros generales aplicables a todos los países miembros. Así, el artículo 6 compromete claramente a todos sus países miembros a adoptar el marco jurídico europeo sobre derechos fundamentales y especificar claramente el estatus jurídico que deberán poseer dichos derechos dentro del sistema legal europeo; esto brinda seguridad jurídica a los sujetos de datos a lo largo y ancho de la unión y posibilita la protección coordinada de dichos datos en el ámbito regional.

Por su parte, el artículo 39 adquiere relevancia al ser examinado el contexto general de la protección de datos dentro del sistema europeo, el cual, como se verá más adelante, establece como límite de la aplicación de sus directivas de protección de datos personales los temas de seguridad nacional y es en la actualidad sumamente escueto al determinar la manera en que deberá de ser regulada la cooperación en materia de

cooperación policial y judicial, la cual requiere la posibilidad de la transmisión transfronteriza de datos personales. Frente a esta situación, dicho artículo permite, por lo menos, coordinar políticas conjuntas en materia de seguridad que nivelen y dirijan dichos esfuerzos.

### *Tratado sobre el Funcionamiento de la Unión Europea*

Segundo de los cuatro documentos que constituyeron materialmente a la Unión Europea, el Tratado sobre el Funcionamiento de la Unión Europea constituye actualmente uno de los textos más antiguos que soportan dicho modelo, siendo firmado originalmente en Roma en 1952 y posteriormente reformado en diversas ocasiones.

Dentro de su texto, el tratado detalla las diversas políticas y acciones que definirán a la Unión, estableciendo en detalle los principios constitucionales y jurídicos que rigen todos los ámbitos de esta (excepto en materia de política exterior, seguridad común y seguridad y defensa), siendo por ello ampliamente aplicado en la práctica jurídica de la Unión.

En materia de protección de datos personales, el Tratado sobre el Funcionamiento de la Unión Europea apunta expresamente en su artículo 16 que:

*"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*

*2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.*

*Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea"* (Unión Europea, 2010).

Dadas las calidades excepcionales del tratado en cuestión, las disposiciones del artículo 16 se tornan fundamentales al garantizar un lugar privilegiado a la protección de datos, dentro del marco de principios legales de la Unión establecido por él; a la vez que eleva el conocimiento de la protección de los datos personales al nivel del Parlamento Europeo y el Consejo de Europa, lo cual posteriormente ha dado lugar a la formulación de las múltiples directivas que se estudiarán a continuación.

Más aún, debe resaltarse que es dentro de dicho artículo donde se establece la necesidad de que la supervisión de la aplicación de dichas normas sea realizada por autoridades independientes, lo cual, tal como se examinará a continuación, se ha visto reflejado en todos los esfuerzos normativos posteriores que sobre el tema ha realizado la Unión.

### *Convenio 108 del Consejo de Europa del 28 de enero de 1981*

Creado por un comité de expertos gubernamentales bajo la autoridad del comité europeo para la cooperación legal y abierto a firma el 28 de enero de 1981 en Estrasburgo, el Convenio 108 del Consejo de Europa es en la actualidad el único instrumento internacional jurídicamente vinculante con potencial para ser aplicado globalmente, dada su apertura a ser adoptado por cualquier país que cuente con la legislación en materia de protección de datos que este requiere.

El convenio procura reforzar la protección de datos mediante la definición de una serie de principios fundamentales reconocidos universalmente, a la vez que establece normas jurídicamente vinculantes y procura la implementación de disposiciones tecnológicamente neutras, capaces de adaptarse a los diversos marcos legales internacionales y aplicables tanto en el ámbito público como en el privado.

De esta manera, el Convenio requiere de los Estados firmantes, su aplicación a los ficheros y tratamientos automatizados de datos de carácter personal realizados por los sectores públicos y privados, a la vez que requiere la adopción de principios de la protección de datos personales como los de tratamiento justo y legal, la adecuación al fin del tratamiento, la relevancia y no exceso de los tos recabados y la limitación del tiempo en que estos puedan ser identificables a un sujeto determinado.

Seguidamente, el convenio procede a establecer límites al tratamiento de algunos tipos de datos (categorías especiales de datos), disposiciones sobre seguridad de estos (requiriendo la adopción de los principios de seguridad de la información) y la formulación de salvaguardas adicionales para el sujeto de datos que le permitan identificar la existencia de un archivo de datos personales, su propósito, la identidad

de quien realiza el tratamiento, y la posibilidad de exigir remedios que incluyan la rectificación, destrucción o modificación de los datos; así como la capacidad de incoar procesos judiciales y administrativos contra todo responsable o encargado del tratamiento que incumpla sus responsabilidades (Consejo de Europa, 1981).

El convenio establece la obligación de los Estados de establecer sanciones y remedios apropiados a la vez que abre la puerta para que estos promulguen normativa tendiente a brindar mayor protección a los datos personales si así lo desean. Asimismo, a partir de su artículo 12, el Convenio establece disposiciones específicas en materia de flujos transfronterizos de datos personales, obligando a los Estados miembros a cooperar en materia de asistencia mutua y la asistencia a los sujetos de datos residentes en el extranjero.

En tanto el Convenio 108 sirve de marco de referencia para más de 43 países en materia de protección de datos, su importancia en la actualidad no puede ser menospreciada, especialmente en tanto el marco jurídico unificado que este propone ha permitido el intercambio de ideas entre los países miembros y la formulación conjunta de mejores prácticas y nuevas normas que afectan tanto a los sectores públicos como privados.

### *Protocolo adicional al Convenio 108 del Consejo de Europa del 8 de noviembre de 2001*

Relativo a las autoridades de control y a los flujos transfronterizos, el Protocolo adicional procura mejorar la aplicación de los principios del Convenio, mediante la

inclusión de provisiones vinculantes necesarias frente al incremento en el intercambio de datos personales, causado por los mercados globalizados y el progreso tecnológico.

Frente a tal situación, el Protocolo crea autoridades supervisoras: entes investigativos y de intervención, capaces de incoar procesos judiciales (dentro de un marco de completa independencia) en respuesta a las reclamaciones de cualquier persona dentro de sus respectivas competencias (Consejo de Europa, 2001).

Asimismo, el Protocolo regula con mayor detenimiento los flujos transfronterizos de datos personales a países no miembros, estableciendo nuevamente la obligación de supervisión y la obligación de que dichas transferencias solamente sean realizadas cuando se asegure un nivel adecuado de protección, o cuando el Derecho interno lo permita con miras a proteger intereses concretos del afectado, por intereses legítimos o cuando por medio de cláusulas contractuales se logren asegurar las garantías suficientes.

### Directivas:

#### *Directiva 95/46/EC*

De necesaria referencia en materia de protección de datos, la Directiva 95/46/EC "sobre la protección de los individuos con respecto al procesamiento de datos personales y sobre el libre movimiento de tales datos" fue firmada el 24 de octubre de

1995 y enmendada en el 2003 por el Parlamento Europeo y el Concejo de la Unión Europea (Parlamento Europeo y Consejo de la Unión Europea, 1995).

Basándose en un marco ideológico que considera que los sistemas de procesamiento de datos se encuentran diseñados para servir al hombre y respetar sus derechos, independientemente de su nacionalidad o residencia, la directiva reconoce que los diferentes niveles de protección existentes en el ámbito internacional se constituyen en un obstáculo potencial a la protección de los datos personales, lo cual afecta también a la competencia y a la seguridad.

Ante dicho panorama, la Directiva procura el establecimiento de un marco único (aplicable a datos procesados tanto por medios automatizados como no automatizados) como primer paso hacia la solución de dicho problema, a la vez que *"Requiere a los países europeos establecer leyes comprensivas de protección de datos, estableciendo estándares mínimos para las leyes nacionales llamados usualmente los "ocho principios""* (Bond, 2003, págs. 5-6).

Dichos principios establecidos por la directiva se dirigen a posibilitar la determinación de la validez legal de todo procesamiento de datos, independientemente de la nacionalidad del sujeto de datos afectado, e incluyen disposiciones relativas a temas como la calidad de los datos, la legitimidad de los datos, las categorías especiales de datos, el derecho de información, el derecho de acceso, el derecho de oposición al tratamiento, la confidencialidad, la seguridad, las notificaciones del tratamiento debidas a la autoridad de control y la posibilidad de que el sujeto o sus representantes recurran ante autoridades judiciales.

Gracias a las líneas por ellas establecidas, *"la Directiva 45/96/CE ha sido percibida por años como poseedora de dos atributos fundamentales: el garantizar y proteger el libre tránsito de la información personal y la protección de los derechos y libertades fundamentales de un individuo (desde la perspectiva de la privacidad)"* (Manolescu, 2010). Asimismo, gracias a la naturaleza misma de la Directiva, con el tiempo tales atributos han sido adoptados por las legislaciones nacionales de los países miembros, quienes han sido libres para implementar la directiva de manera consistente con su cultura social y política, e incluso de brindar mayor protección de la que la Directiva requiere.

Frente a las transferencias transfronterizas de datos personales, la Directiva Europea 45/96/EC se caracteriza por establecer restricciones a las transferencias de datos a todos aquellos países cuya legislación nacional no resulte adecuada, por lo cual desde su entrada en vigencia, una gran cantidad de países han procurado reformar sus leyes con miras a ser considerados adecuados (Bond, 2003, pág. 6); sin embargo, uno de los actuales problemas sobre el tema, se relaciona con la inexistencia de parámetros específicos que permitan determinar cuáles elementos son necesarios para considerar adecuada la protección brindada.

Pese a establecer las restricciones anteriormente mencionadas, debe resaltarse que la Directiva establece también excepciones bajo las cuales las restricciones pueden ser ignoradas; tales como que se cuente con el consentimiento no-ambiguo e informado del interesado[138], específico para los datos utilizados; que la transmisión sea realizada en el cumplimiento de una obligación contractual con el sujeto de datos o que se

[138] Debe tomarse en cuenta que dicho consentimiento puede también ser retirado por parte del sujeto de datos.

asegure por parte del exportador de datos que estos contarán con adecuada protección.

Finalmente, debe recordarse que todo exportador de datos debe cumplir con las disposiciones anteriormente mencionadas, especialmente dado que en caso de incumplimiento el exportador de datos se expone a la pérdida de reputación, presunción de buena fe, confianza de su clientela y a dañar seriamente la imagen de su marca. Asimismo, en caso de ser demostrada su responsabilidad, el exportador puede ser sujeto de severas sanciones que incluyen el establecimiento de multas, la apertura de procesos penales (con la consecuencia del establecimiento de multas, el allanamiento de sus archivos y bases de datos, y la imposición de penas de prisión para los oficiales corporativos responsables), la responsabilidad de reparar al sujeto por los daños y perjuicios sufridos, y la posibilidad de que le sean impuestas órdenes de prohibición o restricción al uso de determinados datos, o la transferencia de datos a lugares específicos.

### *Directiva 2002/58/EC*

Creada el 12 de julio del 2002 dentro del marco regulatorio conocido como el "paquete de telecomunicaciones"[139], y específicamente dirigida a suceder y actualizar la directiva 97//66/EC en materias de privacidad y comunicaciones electrónicas, la Directiva 2002/58/EC (también conocida como e-Privacy Directive) estableció

[139] El cual incluye otras cuatro directivas relacionadas con la creación de un marco normativo general para el sector telecomunicaciones, el establecimiento de disposiciones sobre acceso e interconexión, la regulación de las licencias y autorizaciones y las disposiciones relativas al servicio universal.

provisiones cruciales para la creación de confianza por parte del usuario en los servicios de tecnologías de la información y la comunicación.

En este contexto, la presente Directiva se preocupa por establecer los fundamentos regulatorios para el procesamiento de datos en los servicios de comunicación, para lo cual instituye disposiciones relativas a la seguridad del procesamiento, las retenciones de datos[140], las comunicaciones no solicitadas (mejor conocidas como spam, o correo basura), las cookies, los directorios públicos y el establecimiento de controles gubernamentales.

En materia de seguridad del procesamiento, esta Directiva se caracteriza por obligar a todo proveedor de servicios de telecomunicaciones a implementar algunos de los principios básicos de seguridad de la información, tales como el que los datos solamente puedan ser accedidos por personas autorizadas; la protección de los datos de ser destruidos, perdidos o alterados accidentalmente; y la implementación de políticas de seguridad que incluya la necesaria notificación al interesado y al ente controlador ante toda violación sufrida por sus datos (Parlamento Europeo y Consejo de la Unión Europea, 2002).

En lo que respecta a las retenciones de datos que pudieran ser realizadas por los proveedores de servicios de telecomunicaciones, la Directiva 2002/58/EC se caracteriza por adoptar una posición fundamentalmente protectora de la privacidad de los usuarios, al obligar al proveedor a eliminar o anonimizar de sus servidores todos

[140] Este punto no se ha visto afectado por el fallo "C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others" dado el 8 de abril de 2014 que nulifica las disposiciones de la directiva de retención de datos que estudiaremos a continuación (ver: (Comisión Europea, 2014) y (Corte de Justicia de la Unión Europea, 2014), por lo que los países de la región pueden seguir obligando a sus operadores a retener información de acuerdo con las disposiciones de esta Directiva.

aquellos datos personales que ya no fueran necesarios para brindar el servicio o para realizar el cobro de este. Esta Directiva solamente permite la retención de datos en casos especiales (en los que se cumplan los requisitos de necesidad, proporcionalidad e idoneidad con respecto a los fines de una sociedad democrática) con miras a permitir las investigaciones policiales o para salvaguardar la seguridad nacional, la defensa y la seguridad pública.

En cuanto a las comunicaciones no solicitadas, la Directiva procura el establecimiento de un régimen de entrada por solicitud (opt-in) para las comunicaciones electrónicas comerciales, las cuales incluyen mensajes SMS, multimedia, y todo otro tipo de mensaje recibido en cualquier terminal fija o móvil (con ciertas excepciones) con miras a proteger a los usuarios de los problemas de seguridad relacionados con ellos, así como a la tutela de su derecho a no ser molestado.

Con respecto a las cookies, establece la necesidad de todo proveedor de un servicio de información o comunicación de contar con el consentimiento informado por parte de los usuarios de manera previa a la instalación, almacenamiento o acceso de información de la información ubicada en los equipos de estos; dicho ente se constituye responsable de brindar información clara y comprehensiva a sus usuarios, sobre el almacenamiento o acceso de información que habrá de ser realizado por medio de las cookies y favoreciendo métodos de información y aseguramiento del consentimiento amigables con el usuario.

Similares disposiciones establece la Directiva con respecto a los directorios públicos (tales como las guías telefónicas), para los cuales establece la necesidad de contar con

el consentimiento informado del usuario previamente a que este sea registrado. Las disposiciones en este punto abarcan tanto los directorios públicos tradicionales como aquellos en nuevos formatos y que incluyen datos como la dirección electrónica del perfil de los usuarios o de su correo electrónico.

Finalmente, en materia de los controles gubernamentales, la Directiva requiere que los Estados miembros implementen sistemas eficaces de supervisión por parte de las autoridades nacionales, capaces de establecer las penalidades correspondientes a las violaciones que pudieran darse, así como que cuenten con suficientes poderes y recursos para asegurar el cumplimiento de estas.

### *Directiva 2006/24/EC*

Emitida por el Parlamento Europeo y el Consejo de Europa el 15 de marzo del 2006, la Directiva 2006/24/EC sobre "la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE" procura lograr la armonización regional en el establecimiento e implementación por parte de los proveedores de servicios de telecomunicaciones, de políticas de conservación de datos con miras a facilitar las labores de las agencias policiales y de seguridad.

Sumamente criticada dadas las múltiples implicaciones y riesgos que conlleva (Open Rights Group, 2013), la Directiva asume una posición diametralmente opuesta a la

sostenida por la Directiva 2002/58/CE al requerir el almacenamiento de datos de telecomunicaciones por un plazo que puede ir de los seis a los veinticuatro meses, los cuales pone a disposición de las autoridades que cuenten con una orden judicial que legitime el acceso a tales datos.

Particularmente, puede señalarse que la Directiva es aplicable a datos de tráfico y localización, tanto de personas físicas como jurídicas, así como a los metadatos necesarios para identificar a la persona o al usuario (mas no al contenido de dichas comunicaciones) (Parlamento Europeo y Consejo de la Unión Europea, 2006). De esta manera, la Directiva requiere, entre otros, la conservación de todos los datos necesarios para: rastrear e identificar la fuente de una comunicación[141]; identificar el destino de una comunicación[142]; identificar la fecha, hora y duración de una comunicación[143]; identificar el tipo de la comunicación[144]; identificar los equipos de comunicación utilizados por el usuario[145] y aquellos necesarios para identificar la localización del equipo móvil de comunicaciones[146].

La Directiva impone a las entidades de control la obligación de asegurar que los datos solamente serán accedidos por los entes legalmente autorizados. Asimismo, establece

[141] Número de teléfono, nombre y dirección del suscriptor, ID del usuario, ID del usuario y número de teléfono asignado a cualquier comunicación entrante a las redes de telefonía públicas, así como el nombre y la dirección del suscriptor a quien se asigna una dirección IP en el momento de la comunicación.
[142] Números telefónicos marcados, números a los que la llamada es enrutada, nombre y dirección de los suscriptores, id asignada al usuario y al destinatario.
[143] Fecha y hora de inicio y conclusión de una comunicación, fecha y hora de "login" y "logoff" del servicio de acceso a internet junto con la dirección de IP (dinámica o estática) asignada y hora y fecha de "login" y "logoff" del servicio de correo electrónico o de telefonía por internet.
[144] Servicio telefónico o de internet utilizado.
[145] Números telefónicos para telefonía fija, números telefónicos, IMSI e IMEI en telefonía móvil para ambas partes, "Cell ID" de localización en la que se inició el servicio de comunicaciones (para servicios prepago), números telefónicos usados en conexiones por dial-up o DSL o punto final del originador de una comunicación.
[146] Cell ID al inicio de la comunicación y los datos que identifican la localización geográfica de las torres en referencia con su Cell ID durante el periodo de retención.

la obligación de que el ente retenedor deba cumplir con los principios mínimos de seguridad de la información (los datos retenidos deben poseer la misma calidad y seguridad que los de la red, deben de ser sujetos a medidas técnicas y organizacionales adecuadas para proteger los datos; el acceso solo por personal autorizado a los datos retenidos debe ser garantizado; y los datos deben ser destruidos al finalizar el periodo de retención) y la obligación de que estos sean almacenados de manera tal que estos puedan ser transmitidos sin atraso, a la autoridad competente que los requiera.

Finalmente, debe recordarse que esta Directiva fue declarada inválida a partir del fallo "C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others" dado el 8 de abril de 2014 por la Corte Europea de Justicia, la cual consideró que *"al requerir la retención de aquellos datos y al permitir a las autoridades competentes nacionales el acceder a aquellos datos, la directiva interfiere de una manera particularmente seria con los derechos fundamentales a respetar la vida privada y a la protección de los datos personales (…) al adoptar la Directiva de Retención de Datos, el Legislador de la Unión ha excedido los límites impuestos de conformidad con el principio de proporcionalidad (…) y a pesar de que la retención de datos requeridos por la directiva podría ser considerado apropiado para la obtención del objetivo por ella perseguida, la amplia y particularmente seria interferencia de la directiva con los derechos fundamentales estudiados no se encuentra suficientemente circunscrita para asegurar que esa interferencia se encuentra realmente limitada a lo estrictamente necesario"* (Corte de Justicia de la Unión Europea, 2014).

### *Decisión Marco 2008/977/JHA*

Aprobada por el Consejo de la Unión Europea el 27 de noviembre del 2008, la Decisión Marco 2008/977/JAI procura la protección de los derechos de las personas físicas cuando sus datos son tratados, automática o manualmente, para la prevención, investigación, detección o enjuiciamiento de infracciones penales en el marco de la cooperación policial y judicial en materia penal.

Para lograr tal fin, la decisión establece reglas básicas de protección a los derechos, libertades fundamentales y específicamente, a los datos personales transmitidos entre sí o a autoridades o sistemas de información creados en virtud del título VI del Tratado de la Unión Europea (Disposiciones relativas a la cooperación policial y judicial en materia penal).

En primera instancia, la decisión regula el tratamiento de datos en el contexto de la cooperación judicial, para lo cual permite solamente el tratamiento de datos con fines determinados, explícitos y legítimos y conducentes al fin para el cual fueron recogidos. La Decisión procura seguir el ejemplo del resto de la legislación europea, estableciendo que en principio las categorías especiales de datos no puedan ser procesadas, siendo solamente posible tal procesamiento cuando sea estrictamente necesario y se establezcan ciertas garantías mínimas.

Establece la Decisión la necesidad de que la autoridad controladora competente verifique los datos antes de ser transmitidos o puestos a disposición de persona u organismo alguno, debiendo rectificar, actualizar o completar los datos inexactos y registrar o documentar toda transmisión realizada. Por otro lado, se define la necesidad de que los datos personales sean suprimidos, disociados o bloqueados en el

momento en que ya no sean necesarios, siendo revisada periódicamente la necesidad de su almacenamiento.

Con respecto a la transmisión de los datos, la Decisión hace énfasis en el principio de finalidad, dejando sin embargo abierta la posibilidad de que estos sean tratados para fines distintos (prevención, investigación, detección o enjuiciamiento de otras amenazas o infracciones) en casos fundamentados en la seguridad nacional o pública.

Dado que todo Estado puede establecer limitaciones específicas al intercambio de datos, todo Estado miembro receptor deberá respetar estas y solamente podrá transferir los datos a terceros Estados o a organismos internacionales para fines muy concretos y en ciertas circunstancias, previo consentimiento del Estado del que fueran recibidos los datos.

La Decisión también hace referencia a los derechos de los sujetos de datos, los cuales, por regla general deberán ser informados de dicho procesamiento; puede el interesado solicitar confirmación o informe de cuando sus datos hayan sido transmitidos, donde se incluya el destinatario de dicha transmisión y los datos específicos afectados.

A pesar de tal regla general, los Estados miembros podrán, en casos específicos, establecer límites a dicha información (incluso solicitar que el Estado receptor se abstenga de informar al interesado), decisión que deberá ser informada al interesado por escrito junto con los motivos en los que se basa tal limitación y de su derecho a recurrir tal decisión.

El interesado podrá, a su vez, ejercer activamente sus derechos de rectificación, supresión o bloqueo de los datos que le interesen y que considere equívocos y en caso de verse afectado por el tratamiento de datos o por cualquier otra acción incompatible con la Decisión, tendrá derecho a obtener reparación de los daños y perjuicios sufridos, así como a recurso judicial, de considerar que se ha dado una violación a sus derechos.

Finalmente, la Decisión se preocupa por establecer algunas disposiciones sobre la seguridad del tratamiento de los datos, para lo cual asigna a las autoridades de control competentes el aplicar medidas de seguridad generales en todo tratamiento de datos y específicas en el caso de los tratamientos automatizados, dentro de las cuales se encuentran (Consejo de la Unión Europea, 2008):

- Impedir acceso de personas no autorizadas a las instalaciones de tratamiento de datos personales (control de acceso a las instalaciones);
- Impedir que los soportes sean leídos, copiados, modificados o retirados sin autorización (control de los soportes de datos);
- Impedir tanto la introducción como el conocimiento, modificación o supresión sin autorización de datos en los sistemas (control de la conservación);
- Impedir el uso de los sistemas de tratamiento por personas no autorizadas mediante equipos de transmisión de datos (control de la utilización);

- Garantizar que las personas autorizadas para el uso del sistema de tratamiento de datos solo puedan tener acceso a los datos para los que se les ha autorizado (control de acceso);
- Garantizar que sea posible verificar y comprobar a qué organismos se han transmitido o pueden transmitirse o a cuya disposición pueden ponerse datos personales mediante equipos de transmisión de datos (control de las comunicaciones);
- Garantizar que pueda verificarse y comprobarse a posteriori qué datos personales se han introducido en los sistemas de tratamiento automatizado de datos y en qué momento y por qué persona han sido introducidos (control de la introducción);
- Impedir que durante la transmisión de los datos personales y durante el transporte de soportes de datos, los datos puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);
- Garantizar que los sistemas utilizados puedan repararse en caso de fallo del sistema (recuperación);

- Garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que los datos conservados no se degraden por fallos de funcionamiento del sistema (integridad).

*Directiva 2009/136/EC*

Adoptada por el Parlamento Europeo y el Concejo de la Unión Europea el 25 de noviembre de 2009, la Directiva 2009/136/EC viene a modificar las directiva 2002/58/CE, mediante el reforzamiento de las disposiciones ya existentes en materia de consentimiento para la instalación de cookies en los equipos de los usuarios (Parlamento Europeo y Consejo de la Unión Europea, 2009).

Específicamente, esta Directiva considera el consentimiento informado como elemento fundamental que determinará la capacidad de una página para la instalación de cookies. Y establece como única excepción el que la cookie en cuestión sea absolutamente necesaria para la satisfacción del servicio que ha sido solicitado por el usuario, o cuando el almacenamiento de la información se deba solamente al propósito de efectuar una comunicación en línea.

Por otro lado, esta Directiva modifica la 2002/58/EC mediante la modificación de algunas de las definiciones (datos de localización y violación de datos personales), la inclusión de disposiciones en materia de seguridad de la información, y el establecimiento de las acciones específicas por tomar de parte de todo proveedor de servicios de comunicaciones electrónicas, frente a una violación de datos personales.

Asimismo, establece la Directiva la capacidad de las autoridades nacionales competentes de dictar directrices y mayores instrucciones sobre el procedimiento por seguir frente a una violación de datos personales y de realizar auditorías para asegurarse del cumplimiento de estas.

Finalmente, la Directiva refuerza las disposiciones ya existentes sobre comunicaciones no solicitadas, estableciéndose la imposibilidad de utilizar sistemas de llamada

automática y comunicación sin intervención humana sin consentimiento previo; se prohíbe también el envío de mensajes electrónicos para venta directa que oculten la identidad del remitente, estableciéndose así la necesidad de establecer en toda comunicación electrónica un método sencillo y gratuito para que el usuario pueda oponerse a la utilización de su información, tanto en el momento de su recopilación, como en todo mensaje que este reciba a posteriori.

## Regulación

### *Regulación (EC) 45/2001*

Promulgada el 18 de diciembre del 2000, la Regulación 45/2001 sobre "la protección de los individuos con respecto al procesamiento de datos personales por las instituciones y cuerpos de la comunidad y sobre el libre movimiento de tales datos", procura el aseguramiento de un alto nivel de protección de los datos en un marco que asegure el cumplimiento de los principios básicos de la protección de datos, a la vez que establece la Autoridad Europea de Protección de Datos (Parlamento Europeo y Consejo de la Unión Europea, 2000).

Según las estipulaciones de la Regulación, la Autoridad Europea de Protección de Datos se constituye como una autoridad independiente, equiparable a las autoridades nacionales de protección de datos, responsable de monitorear la aplicación correcta

de la normativa sobre protección de datos personales por parte de las instituciones y entes de la Unión.

La Regulación establece también la necesidad de que toda institución y ente de la Unión Europea cuente con un *oficial de protección de datos*, encargado de cooperar con la Autoridad Europea, con miras a garantizar los derechos de los sujetos de datos. Asimismo, dado el carácter vinculante de los derechos reconocidos a los sujetos de datos a lo largo de la Unión, la regulación reconoce la capacidad de tales sujetos de interponer quejas directamente ante la Autoridad Europea de Protección de Datos.

### Reformas Propuestas

El proceso de reforma legislativa del marco de protección de datos vigente en Europa, propone fundamentalmente una actualización de las piezas normativas que sirven de base a dicho sistema: la Directiva 95/46/EC y la Decisión Marco 2008/997/JHA, mediante la promulgación de nuevas directrices generales sobre protección de datos, y un reglamento general para la protección de aquellos datos personales que sean utilizados en el contexto de las investigaciones policiales.

Tomando en consideración los objetivos fundamentales de dichas herramientas (la protección del derecho fundamental a la protección de datos y el aseguramiento del libre tránsito de los datos personales entre los Estados miembros), y considerando la necesidad de evitar fragmentación en la implementación de la protección de datos a lo

largo de la Unión, en la actualidad la Unión Europea se encuentra dando los pasos finales a lo que esperan será un marco normativo coherente y de fácil implementación.

Basada en las metas planteadas por la estrategia "Europa 2020" que forma parte de la Agenda Digital para Europa, y tomando en consideración innumerable cantidad de estudios realizados desde los inicios del Sistema Europeo de Protección de Datos Personales, la reforma legislativa procura el cumplimiento de tres objetivos fundamentales: mejorar las dimensiones comerciales internas de la protección de datos, hacer más efectivo el ejercicio de los derechos de protección de datos por los individuos y crear un marco comprehensivo y coherente que cubra la totalidad de las áreas competencia de la Unión (incluyendo áreas actualmente casi desprotegidas como lo son la cooperación policial y judicial) (Parlamento Europeo, 2013).

En este contexto, las propuestas realizadas procuran la implementación de cambios moderados (tendientes a la búsqueda de soluciones específicas a los problemas encontrados en el modelo vigente actualmente) que conlleven mejorías importantes en materia de certeza legal para todos los interesados, reducción de cargas administrativas y consistencia de la protección a lo largo de la Unión.

### *Propuesta de Reglamento General de la Protección de Datos 2012/0011(COD)*

Basada fundamentalmente en los artículos 16(2) y 114(1) del Tratado de Funcionamiento de la Unión Europea, la propuesta realiza una relectura de la protección de datos utilizada por la Directiva 95/46/EC, con miras a su actualización y

mejoramiento. Para lograr tales objetivos, la propuesta de Reglamento General reitera los principios ya existentes en la materia, a los cuales añade elementos nuevos, tales como el principio de transparencia, la clarificación del principio de minimización de datos y el establecimiento de responsabilidad para el controlador; a la vez que establece claramente los criterios determinantes para el procesamiento conforme con la ley de los datos personales (balance de intereses y cumplimiento con obligaciones legales e interés público).

Con respecto a los derechos de los usuarios, la propuesta establece la obligación del controlador de proveer información durante (y relevante a) todas las etapas de tratamiento, la cual debe ser transparente, accesible y comprensible al sujeto de datos. Asimismo, requiere el establecimiento de medios de ejercicio de los derechos de los sujetos de datos que contemplen las peticiones electrónicas y que sean respondidos dentro de un plazo determinado, de manera motivada.

La propuesta propone también cambios como la determinación de los derechos de los menores de edad frente al tratamiento de sus datos (así como las condiciones para que tal tratamiento sea legítimo); la especificación de las obligaciones del controlador con respecto al sujeto; la aclaración de aspectos relativos a los derechos de acceso, rectificación, destrucción, objeción, al olvido y a establecer quejas en contra del controlador en caso de que esto sea necesario (Comisión Europea, 2012).

La propuesta detalla las obligaciones del controlador en materia de responsabilidad (accountability), asignando la carga de la prueba a este, quien deberá, mediante la adopción de políticas y mecanismos internos, asegurar el cumplimiento de los

principios de la protección de datos desde el diseño de sus sistemas (privacy by design). Asimismo, deberá demostrar el cumplimiento de su obligación de documentar correctamente todo procesamiento; la implementación de medidas de seguridad apropiadas; la notificación de las violaciones sufridas por los datos personales bajo su responsabilidad y su obligación de llevar a cabo estudios de impacto con anterioridad a realizar operaciones riesgosas (Parlamento Europeo, 2013).

Adicionalmente a los elementos anteriormente destacados, la propuesta crea la figura del "delegado de protección de datos", figura independiente encargada de la fiscalización interna de la materia cuya existencia será obligatoria en el sector público y en el sector privado que supere ciertos criterios (empresas de gran tamaño o empresas cuyas actividades requieran monitoreo regular y sistemático).

Estos delegados deberán trabajar en cooperación con las autoridades de supervisión nacionales (a las cuales asigna claros requisitos de independencia implementando jurisprudencia del Tribunal de Justicia de la Unión Europea (Parlamento Europeo, 2013)). Tal requisito de cooperación es extendido también a las diversas autoridades de supervisión, a las cuales asigna consecuencias en caso de no cumplir con solicitudes provenientes de sus pares, a la vez que introduce mecanismos de consistencia y crea la Junta Europea de Protección de Datos.

En materia de transferencias transfronterizas de datos personales, el nuevo reglamento aclara puntualmente los criterios, condiciones y procedimientos requeridos para aceptar el nivel de protección brindado por un país como adecuado o no adecuado (requiriendo la existencia de legislación sobre el tema, la posibilidad de

obtener reparación judicial por las afectaciones y la independencia de los entes supervisores). Asimismo, establece como requisito para toda transferencia a terceros países que no cuenten con dicha adecuación, la implementación de cláusulas contractuales estándar y de reglas corporativas vinculantes (Parlamento Europeo, 2013).

Finalmente, la propuesta es clara al establecer los remedios, la responsabilidad y las sanciones relacionadas con todo tratamiento de datos personales. En este punto, el nuevo reglamento asegura el derecho, tanto del sujeto de datos como de organizaciones u asociaciones creadas para tal fin, de establecer quejas ante el ente supervisor en caso de violaciones de datos. Más aún, establece la posibilidad de tales actores de establecer procesos judiciales tanto en contra del controlador o procesador de datos, como en contra del ente supervisor, dirigidas a obtener reparaciones o a obligarlos a actuar en un caso determinado.

### *Propuesta de Directiva del Parlamento Europeo y del Consejo 2012/0010(COD)*

Dirigida al mejoramiento de la regulación existente en materia de protección de datos en el área de la cooperación policial y judicial en asuntos criminales, la Propuesta de Directiva del Parlamento Europeo y del Consejo procura eliminar los vacíos existentes en la Decisión Marco 2008/97/JHA.

Basada fundamentalmente en el artículo 16 del Tratado de Funcionamiento de la Unión Europea y en el Programa de Estocolmo formulado por la comisión Europea, la

propuesta crea un marco legal nuevo, capaz de regular la protección de datos en el área de la cooperación policial y judicial, tanto en el ámbito interno de la Unión Europea (y de cada uno de los países miembros) como en el ámbito de la cooperación interinstitucional e internacional.

La propuesta da inicio estableciendo los principios del procesamiento de datos personales, para lo cual distingue a los sujetos de datos en diversas categorías, siguiendo el ejemplo de normas similares vigentes para Europol y Eurojust (Comisión Europea, 2012, pág. 9).

Más adelante, la propuesta establece los derechos del interesado, los cuales incluyen su derecho a recibir información clara y gratuita por parte de los Estados miembros y demás procesadores, sobre el tratamiento realizado a sus datos, a la vez que reitera el derecho de todo sujeto de dato a ejercer sus derechos (especialmente el derecho de acceso) de manera gratuita, limitado solamente por las medidas legítimas basadas en la naturaleza específica del procesamiento realizado.

La propuesta regula también las obligaciones de los controladores de datos, a quienes asigna la obligación de cumplir con los principios de protección de datos y de seguridad de la información, los cuales deben ser implementados desde el mismo diseño del sistema de tratamiento. Por otro lado, regula también las relaciones entre los responsables del tratamiento (autoridad pública competente) y los encargados del tratamiento (ente u organismo que trate datos personales por cuenta del responsable del tratamiento), estableciendo como corresponsable a todo encargado del tratamiento que se exceda en sus funciones.

Especifica por otra parte esta propuesta el papel que deberán adoptar las autoridades nacionales de supervisión, cuyas competencias incluirán la atención e investigación de quejas interpuestas por sujetos de datos, realizar labores de asistencia mutua en conjunción con sus pares internacionales y ejercer el derecho de acceso en nombre de los sujetos de datos con miras a cerciorarse de la legalidad del procesamiento de datos realizado.

La propuesta asigna también a los responsables del procesamiento las obligaciones de notificar violaciones de datos a los sujetos de datos afectados y de contar con un oficial de protección de datos, quienes a su vez deben informar y coordinar con los entes supervisores nacionales para encontrar soluciones a dichas violaciones.

Las transferencias de datos a terceros países solamente podrán ser realizadas en tanto sean necesarias para la prevención, investigación, detección, o persecución de delitos (o en caso de que sean necesarias para la ejecución de la pena); sin embargo solamente podrán ser realizadas a países sin protección adecuada cuando se tomen las medidas necesarias para garantizar la protección de los datos.

Finalmente, la propuesta aborda el tema de los remedios, responsabilidades y sanciones de la misma manera en que lo hace la propuesta para el Reglamento General, permitiendo al sujeto establecer sus quejas a nivel judicial o administrativo y obtener compensación por las afectaciones sufridas, a la vez que establece las penas aplicables a las violaciones a la Directiva.

### *Modelo Estadounidense*

Tal como se estudiara con anterioridad, el sistema legal de Estados Unidos de América (basado en el common law inglés), posee una percepción distinta de la privacidad que la existente en los países de tradición civilista. Tal diferencia, aunada con los ideales liberales que han caracterizado al gobierno estadounidense en las últimas décadas, ha tenido como consecuencia la generación en ese país de un sistema "diametralmente opuesto al sistema europeo" (Guadamuz, 2000), en el cual se ha evitado, por lo general, la regulación gubernamental de las políticas de privacidad y protección de datos, y en su lugar se ha optado por fomentar un modelo de autorregulación (o regulación mínima).

Esta particularidad del modelo estadounidense puede ser explicada siguiendo a Kirsh, Philips & McIntyre, quienes afirmaran que *"Pese a que los norteamericanos son agudamente sensibles sobre su privacidad en el ciberespacio, también son reacios a empoderar al gobierno para que proteja su privacidad. (…) La demanda del consumidor debería guiar a los proveedores hacia la promoción de sus medidas de protección a la privacidad en un esfuerzo por acumular una mayor cuota de mercado sobre aquellos competidores que no ofrezcan medidas similares"* (Kirsh, Philips, & McIntyre, 1996).

Así como lo manifiestan los autores supracitados, el sistema de autorregulación o regulación mínima deja a disposición de las empresas y de los consumidores la toma de decisiones en materia de protección de datos y procura evitar la intervención estatal en donde esta no sea absolutamente necesaria. A pesar de tal situación, el

marco legislativo (tanto federal como estatal)[147] existente en dicho país, cuenta actualmente con una gran cantidad de legislación y jurisprudencia relacionada con la protección de la privacidad y los diversos tipos de datos personales[148].

Con miras a brindar al lector una idea del contexto normativo actual que moldea el modelo estadounidense de privacidad y protección de datos personales, a continuación se estudiará la legislación federal[149] más relevante, mencionando brevemente las particularidades de cada norma.

## Legislación Federal Relevante

### *Americans with Disabilities Act of 1990*

(Congreso de los Estados Unidos de América, 1990)

Instituida como ley federal por el Congreso de los Estados Unidos el año de 1990, la Americans with Disabilities Act (ADA) procura la protección de los ciudadanos discapacitados, mediante la ampliación de sus derechos civiles para evitar y prohibir la discriminación contra ellos. Define la discapacidad como un "impedimento físico o mental que limita substancialmente una actividad importante de la vida" (Congreso de los Estados Unidos de América, 1990).

[147] Debe recordarse al lector que en el sistema de Common Law, tanto los Estados como el Gobierno Federal poseen la capacidad de crear leyes vinculantes para sus habitantes. Asimismo, es necesario indicar que el sistema legal estadounidense se basa en gran medida en la solución casuística de los problemas encontrados, la cual forma jurisprudencia vinculante.
[148] Especialmente con respecto a los datos financieros.
[149] El presente trabajo se limitará únicamente al estudio de la legislación federal con miras a brindar al lector una mirada introductoria a la normativa aplicable; no se detendrá a analizar la legislación estatal ni mucho menos la jurisprudencia relevante, por motivos de espacio.

Específicamente, la ADA se relaciona con la protección de datos personales en tanto establece disposiciones específicas dirigidas a la protección de la información médica de los individuos, frente al mal uso de los datos médicos por empleadores potenciales; estos solamente podrán solicitar exámenes médicos si todos sus empleados son sometidos a ellos y la información recabada es clasificada y tratada como información confidencial.

### *Bank Secrecy Act of 1970*

(Congreso de los Estados Unidos de América, 1970)

Instituida como ley federal por el Congreso de los Estados Unidos durante el año de 1970, la Bank Secrecy Act (BSA o Currency and Foreign Transactions Reporting Act) procura detectar y prevenir el delito de lavado de dinero en las instituciones financieras estadounidenses, por medio del establecimiento obligaciones específicas para dichos entes. Específicamente, la BSA requiere que las instituciones financieras mantengan registros detallados de las transacciones bancarias realizadas y se encarguen de reportar la actividad sospechosa que pudiese relacionarse con los delitos anteriormente mencionados.

Evidentemente, esta ley se relaciona específicamente con los datos financieros de los ciudadanos estadounidenses, específicamente con los reportes sobre transacciones monetarias, los reportes sobre transacciones de instituciones financieras extranjeras y los reportes sobre la importación y exportación de divisas. Tales reportes y documentos generados a partir de su aplicación son muy utilizados por las fuerzas de

seguridad nacionales y extranjeras en su lucha contra la delincuencia organizada y la legitimación de capitales.

### *Cable Communications Privacy Act of 1984*

(Congreso de los Estados Unidos de América, 1984)

Conocida comúnmente como la "Cable Act", fue instituida como ley federal por el Congreso de los Estados Unidos durante el año de 1984, con vistas a proteger la información personal de los suscriptores de televisión por cable dentro de los Estados Unidos, al prohibir la publicación de tal información, a la vez que permite a los usuarios verificar su información.

Asimismo, la Cable Act incluye disposiciones relativas a las notificaciones debidas al usuario (que incluirán la naturaleza de la información recopilada, información sobre las publicaciones que pudieran hacerse de tal información, el tiempo durante el cual esta información podrá ser guardada, entre otros) y establece que el operador solamente podrá recopilar información personalmente identificable para prestar un servicio o para detectar la recepción no autorizada de las comunicaciones por cable.

Finalmente, la Cable Act contempla tanto el derecho de acceso a la información por parte del usuario (e incluso el derecho de corregir cualquier error), como la obligación del operador de destruir toda información personalmente identificable que ya no sea necesaria. Asimismo, la ley establece las bases con las cuales un operador podrá publicar la información recopilada, siendo una de ellas la cesión de información a una entidad gubernamental, tras recibir orden judicial, con fines de facilitar los procesos

judiciales (siempre y cuando al sujeto se le brinde la oportunidad de apelar y contestar las acusaciones en su contra).

### *Children's Internet Protection Act of 2000*

(Congreso de los Estados Unidos de América, 2000)

Promulgada en el año 2000 con el objetivo de proteger a la niñez frente al contenido obsceno o peligroso de la red, la Children's Internet Protection Act (CIPA) impone obligaciones determinadas a las escuelas y bibliotecas estadounidenses que apliquen a descuentos especiales en las tarifas de conexión a Internet, ofrecidas por los diversos programas estatales o federales creados para tal fin.

Con miras a asegurar tal protección, las escuelas y bibliotecas deberán adoptar e implementar políticas de seguridad en internet que incluyan medidas sobre *"(a) el acceso de menores de edad a contenidos inapropiados en Internet; (b) la seguridad y protección de los menores cuando utilizan correo electrónico, salas de chat y otras formas de comunicaciones electrónicas directas; (c) acceso no autorizado, incluyendo el llamado "hackeo", así como otras actividades ilegales por menores en la red; (d) revelación, uso y diseminación no autorizadas de información personal con respecto a menores de edad; y (e) medidas que restrinjan el acceso de los menores a los materiales que les puedan resultar dañinos"* (Federal Communications Commision, 2013).

De esta manera, se puede observar cómo en el ámbito de la protección de datos personales CIPA hace referencia fundamentalmente a la protección de la totalidad de los datos de las personas menores de edad. Asimismo, debe resaltarse que esta ley no

requiere que el tráfico de internet sea rastreado de ninguna manera por parte de la institución.

### *Children's Online Privacy Protection Act of 1998*

(Congreso de los Estados Unidos de América, 1998)

Constituida como ley federal por el Congreso de los Estados Unidos de América el 21 de octubre de 1988, la Children's Online Privacy Protection Act (COPPA) se encuentra dirigida fundamentalmente a la protección de la privacidad de los usuarios menores de edad del internet. Específicamente, esta ley regula a las personas o entidades ubicadas dentro de la jurisdicción estadounidense que recopilen información de personas menores de 13 años de edad, lo cual realiza por medio del establecimiento de diversas disposiciones cuyo acatamiento es supervisado por la Comisión Federal de Comercio (Federal Trade Commission o FTC).

A partir de su última enmienda, realizada el 12 de diciembre de 2012, COPPA requiere que todo ente que pretenda o sepa que recopila o procesa datos personales (incluyendo identificadores persistentes del usuario, imágenes, videos, datos de geolocalización, e incluso metadatos) de una persona menor de 13 años de edad, deba cumplir con los siguientes requisitos:

*"1. Publicar una política clara y comprehensiva en materia de privacidad en línea describiendo sus prácticas de información para información personal recopilada a partir de los menores de 13 años; 2. Hacer esfuerzos razonables (tomando en consideración la tecnología existente) para proveer notificación directa a los padres sobre las prácticas del operador con respecto a la*

*recolección, uso o liberación de datos personales de niños menores de 13 años, incluyendo notificación de cualquier cambio material a las prácticas anteriormente aprobadas por los padres; 3. Obtener consentimiento verificable de los padres, con limitadas excepciones, antes de cualquier recolección, uso y/o publicación de datos personales de niños menores de 13 años; 4. Proveer medios razonables para que los padres revisen los datos personales recopilados a partir de sus hijos y para rehusar a permitir futuros usos o mantenimiento de tales datos; 5. Establecer y mantener procedimientos razonables para proteger la confidencialidad, seguridad e integridad de la información personal recolectada de niños menores de 13 años, incluyendo el tomar pasos razonables para revelar/liberar tal información solamente a aquellas partes capaces de mantener su confidencialidad y seguridad; y 6. Retener los datos personales recolectados a partir de un niño tan solo por el tiempo necesario para cumplir el propósito para el cual estos fueron recolectados y borrar la información usando medidas razonables para protegerla contra usos o accesos sin autorización"* (Larose & Siripurapu, 2013).

Se debe resaltar que a pesar de las enmiendas recientemente realizadas, la ley en cuestión aún posee algunos vacíos, viéndose por ejemplo limitada su aplicación con respecto a las aplicaciones móviles ("apps"), a las redes sociales y a las tiendas de aplicaciones móviles. Tales vacíos se han aunado con una innegable falta de aplicación de la ley[150] en la industria, para causar gran malestar, críticas y controversia entre el pueblo estadounidense, al considerarse incluso que la gran cantidad de limitaciones que establece afectan negativamente el derecho a la libertad de expresión de los menores de edad.

[150] Causada fundamentalmente por la dificultad que implica para el operador de un servicio web de verificar la edad del usuario para luego identificar y contactar al padre del mismo y obtener una muestra verificable de consentimiento de este.

### *Computer Fraud and Abuse Act of 1984*

(Congreso de los Estados Unidos de América, 1984)

Originalmente promulgada por el Congreso de los Estados Unidos como una enmienda a la *ley de fraudes* y posteriormente enmendada en los años de 1994 y 2001, la Computer Fraud and Abuse Act (CFAA) prohíbe los ataques a sistemas informáticos (especialmente a aquellos relacionados con computadores federales, bancarios y aquellos conectados a la internet) que busquen acceder, amenazar, dañar, espiar o utilizar dichos sistemas como medios para realizar fraudes.

Sumamente relacionada con el ámbito de la ciber-seguridad, la CFAA contempla e impone severas penas a quienes cometan las siguientes actividades (McAfee, Inc., 2013):

- Obtener información sobre seguridad nacional.
- Comprometer la confidencialidad de una computadora.
- Acceder sin autorización a una computadora gubernamental.
- Acceder a una computadora para defraudar y obtener valores.
- Transmisión voluntaria y daños intencionales a un sistema informático.
- Acceder intencionalmente y causar daños intencionales a un sistema informático.
- Acceder intencionalmente y causar daños temerarios a un sistema informático.
- Tráfico de contraseñas y extorción con amenazas de daño a las computadoras.

La CFAA procura a su vez la protección de la información financiera, estatal o privada, frente a las amenazas informáticas anteriormente mencionadas, posibilitando a toda

persona afectada por actos contrarios a sus disposiciones a establecer acciones civiles contra el autor de dichos actos.

### *Communications Assistance for Law Enforcement Act of 1994*

(Congreso de los Estados Unidos de América, 1994)

Creada en respuesta a las dificultades encontradas por las autoridades a la hora de vigilar por los medios legalmente válidos las telecomunicaciones digitales e inalámbricas, la Communications Assistance for Law Enforcement Act de 1994 (CALEA) busca facilitar las escuchas telefónicas al obligar a los operadores a rediseñar la arquitectura de sus redes de telecomunicaciones.

Caracterizada por contar con disposiciones abiertas en cuanto a los sistemas exactos que deberán utilizar los operadores de red para posibilitar las escuchas de sus redes, CALEA asigna individualmente a cada operador la responsabilidad de diseñar sus propios sistemas o adherirse a los estándares y soluciones creados por la industria, siempre y cuando reporten el sistema utilizado ante la Comisión Federal de Telecomunicaciones.

Debe señalarse que si bien el texto original de CALEA establece que sus disposiciones no son aplicables a los servicios de información ni a los sistemas dirigidos únicamente a la interconexión de redes (y por extensión a los datos que viajan por el internet), dicha ley si hace referencia a los servicios de computación remota (equivalente actual a la computación en la nube), los cuales sí deberán adaptarse a sus disposiciones, por lo

que el operadores deberá brindar datos a las entidades gubernamentales que lo soliciten.

En términos generales, si bien CALEA se limita a facilitar las escuchas telefónicas tradicionales, su articulado afecta los datos personales (y especialmente los metadatos) al disponer que los registros del operador de telecomunicaciones, incluyendo el nombre, la dirección, los recibos telefónicos, el número telefónico o la forma de identificación del suscriptor y la duración del servicio brindado (McAfee, Inc., 2013) deberán ser comunicados a aquellas agencias gubernamentales que lo requieran con fundamento en una orden judicial.

Finalmente, debe apuntarse que esta ley federal estadounidense ha sido interpretada de manera cada vez más amplia, viéndose incluidos dentro de su ámbito de aplicación a los proveedores de acceso a internet de banda ancha basados en infraestructura y a los operadores u proveedores de servicios de *Voz sobre Protocolo de Internet* (VoIP) (Federal Communications Commision, 2013); por lo que la preocupación sobre la ampliación y potencial aplicación de esta ley para recopilar datos de internet ha crecido en los últimos años (Electronic Frontier Foundation, 2013).

### *Computer Matching and Privacy Protection Act of 1998*

(Congreso de los Estados Unidos de América, 1988)

Formulada por el congreso estadounidense el año de 1988 como una reforma a la Privacy Act de 1974, la Computer Matching and Privacy Protection Act busca establecer salvaguardas y proteger la intimidad de los administrados frente a las

nuevas tecnologías de la información que permitían no solamente recoger grandes cantidades de datos, sino también procesarlos y compararlos.

Específicamente, la Computer Matching and Privacy Protection Act responde a una técnica mediante la cual los datos personales eran comparados y unidos; sin embargo, su aplicación se limita solamente a aquellos datos mantenidos en un sistema protegido bajo las disposiciones de la Privacy Act, que sean emparejados con datos de sistemas de beneficios federales y/o datos de registros de personal o nóminas de sueldos federales.

Esta ley estableció la obligación de las agencias federales estadounidenses de llevar a cabo solamente aquellos programas de emparejamiento de datos que fueran negociados por escrito y aprobados por la junta respectiva (Junta de Integridad de Datos). Asimismo, requería que las agencias en cuestión reportaran detalladamente los programas realizados ante el Congreso, a la vez que debían notificar a los aplicantes y beneficiarios de los programas anteriormente mencionados que sus datos podrían ser sujetos a dicho procesamiento (Privacilla.org, 2001).

*"La ley cubre los "registros", lo que significa "cualquier ítem, colección, o grupo de información sobre un individuo que sea mantenida por una agencia, incluida, pero no limitada a educación, transacciones financieras, historial médico e historial criminal o de empleo y que contenga el nombre o el número identificador, símbolo u otro identificador particular asignado al individuo, tal como una huella digital, una impresión de voz o una fotografía"* (McAfee, Inc., 2013).Y sobre ellos brinda a los sujetos de datos el derecho a un debido proceso, evitando que las agencias tomen medidas que les perjudican sin antes verificar por su propia cuenta los resultados del procesamiento y les notifique con treinta días de antelación.

Finalmente, puede considerarse, en opinión del suscrito autor de esta investigación, que el resultado del presente análisis de la Ley deberá apegarse a la opinión manifestada por el proyecto "Privacilla" cuyos miembros consideran que *"a pesar de que la Computer Matching and Privacy Protection Act ciertamente involucra procedimientos detallados, incluyendo a las obscuras "Juntas de Integridad de los Datos", es probablemente más notable por el hecho de que institucionalizó el intercambio de datos entre las agencias gubernamentales federales. La información recabada para un propósito puede ser utilizada para diferentes propósitos por una agencia federal diferente. Pese a que la integridad y la justicia parecen ser aseguradas por la Ley, la privacidad no lo es" (Privacilla.org, 2001).*

### *Consumer Credit Reporting Reform Act of 1996*

(Congreso de los Estados Unidos de América, 1996)

Constituida como ley federal durante el año de 1996,la Fair Credit Reporting Reform Act procuraba reformar la Fair Credit Reporting Act, con miras a brindar protección adicional a los trabajadores y a sus datos crediticios. Lo anterior en tanto resultaba común práctica el que sus potenciales empleadores obtuvieran copias de sus informes crediticios y los emplearan para decidir si habrían de contratar al sujeto o si ya contratado, debían tomar medidas que le afectaran con base en un examen de dichos reportes.

La reforma fundamentalmente requiere que todo empleador que realice chequeos de crédito en sus empleados deba notificar sus intenciones de obtener una copia del reporte crediticio del empleado y solicitar una autorización por escrito para ello. Asimismo, el empleador deberá brindar copia del reporte obtenido al sujeto de datos

y, en caso de que decidiera ejercer acción alguna con base en lo establecido en el reporte en cuestión, debe brindar también al empleado copia de los derechos establecidos por esta ley.

### *Drivers Privacy Protection Act of 1994*

(Congreso de los Estados Unidos de América, 1994)

Promulgada por el Congreso de los Estados Unidos durante el año de 1994 con miras a proteger la información recopilada por las agencias estatales de vehículos automotores, la Drivers Privacy Protection Act (DDPA) prohíbe la comunicación o revelación de los datos personales relacionados con los registros de vehículos ni aquellas informaciones personales "altamente restringidas" (la fotografía o imagen de un individuo, su número de seguridad social y la información médica del sujeto).

A pesar de ello, la ley contempla ciertos usos aceptables, tales como aquellos usos necesarios de la información realizados por agencias gubernamentales, el uso de los datos en conexión con asuntos de registro, seguridad automotriz, examen de emisiones del vehículo, examen de las partes y los vendedores autorizados, y actividades de investigación del mercado de automotores.

Asimismo, son permitidos los usos de la esta información por un negocio legítimo (para verificar la información proporcionada por el usuario o para actualizarla) y para su uso en procedimientos civiles, penales, administrativos o arbitrales, a la vez que se admite su uso en actividades de investigación, aseguramiento, notificación, investigación y asuntos laborales, entre otros.

Tal como puede verse, la ley en cuestión en realidad brinda una protección relativamente laxa a la información personal del conductor o dueño de un vehículo automotor, limitando realmente su enfoque a las actividades de las diversas administraciones estatales, pero permitiendo actividades tales como la reventa de la información recopilada para fines similares a los permitidos. A pesar de ello, con el paso del tiempo esta ley ha sido enmendada con miras a la limitación de algunos de sus defectos[151].

### *Electronic Communications Privacy Act of 1984*

(Congreso de los Estados Unidos de América, 1984)

Creada en 1984 con el espíritu de una ley novedosa y progresiva dirigida al establecimiento de estándares en materia de privacidad de las comunicaciones electrónicas en los Estados Unidos (Center for Democracy & Technology, 2013), la Electronic Communications Privacy Act (ECPA) es un estatuto federal que aborda fundamentalmente el problema del monitoreo gubernamental de las comunicaciones realizadas por medio de telefonía móvil y el internet.

Dentro de su articulado, la ECPA establece provisiones sobre el acceso, uso, revelación, interceptación y protección de la privacidad de las comunicaciones electrónicas (McAfee, Inc., 2013), las cuales entiende como *"cualquier transferencia de signos, señales, escritura, imágenes, sonidos, datos o inteligencia de cualquier naturaleza transmitida en su totalidad o en parte por sistemas cableados, de radio, electromagnéticos, foto-electrónicos o*

[151] Así por ejemplo, la última enmienda de la que se tiene noticia a la fecha se dirigió a requerir que los estados soliciten el permiso de los individuos antes de vender o liberar su información a vendedores o agencias de publicidad de terceras partes (Electronic Privacy Information Center, 2013).

*foto-ópticos que afecten el comercio interestatal o exterior pero no incluye las comunicaciones orales, las comunicaciones realizadas por tonos, las comunicaciones de dispositivos de rastreo y las transferencias de fondos bancarios realizadas por medios electrónicos"* (Congreso de los Estados Unidos de América, 1984).

La ECPA prohíbe, entre otros, el uso de comunicaciones electrónicas obtenidas sin orden judicial en procesos judiciales para acusar o procesar a un individuo, las escuchas telefónicas sin orden judicial, las interrupciones o intercepciones ilegítimas de las transmisiones de un sujeto y las publicaciones ilegítimas de la información contenida en una comunicación electrónica.

A pesar de tal amplitud y visión original en su redacción, más de 25 años han pasado desde que la ECPA entró en vigencia y la tecnología ha avanzado más allá de lo que los legisladores originales podían prever. A pesar de este cambio que podría parecer natural, el elemento más preocupante es que no ha habido movimientos legislativos dirigidos hacia su actualización, por lo que actualmente importantes cantidades de información personal se encuentran desprotegidas. Tal situación es aprovechada por el gobierno norteamericano, el cual fundamenta en tales vacíos legales su derecho a rastrear los movimientos de ciudadanos y extranjeros por igual e intervenir en los diversos medios de comunicación electrónica.

### *Electronic Freedom of Information Act of 1996*

(Congreso de los Estados Unidos de América, 1996)

Originalmente promulgada por el Congreso estadounidense en el año de 1966, la Freedom of Information Act (FOIA) se dirige a garantizar el Derecho al Acceso a la Información Pública, así como a toda la información gubernamental que verse sobre individuos. La Electronic Freedom of Information Act (E-FOIA) viene a ampliar las disposiciones de la FOIA, estableciendo la necesidad de que todas las agencias estatales publiquen electrónicamente algunos tipos de registros creados a partir de noviembre de 1996.

A pesar de las virtudes de enmienda realizada por E-FOIA, debe reconocerse que en la actualidad las disposiciones de la Freedom of Information Act continúan siendo difícilmente aplicables. Lo anterior en tanto dicha ley incluye en su texto nueve excepciones a la capacidad de un individuo de requerir información, por lo que no es aplicable a: *asuntos designados como Secreto de Estado; datos relacionados con el manejo interno de una agencia; asuntos que por disposiciones legales no puedan ser publicados; información secreta o confidencial de un individuo; memorándums interiores de la agencia (o memorándums entre agencias), datos capaces de afectar la privacidad personal; datos recopilados como parte de un proceso judicial (y que cumplan con ciertas especificaciones); información relacionada con la regulación o supervisión de instituciones financieras; e información geológica o geofísica* (Congreso de los Estados Unidos de América, 1966).

### *Electronic Funds Transfer Act of 1978*

(Congreso de los Estados Unidos de América, 1978)

Creada en 1978 con miras a establecer los derechos y responsabilidades de los participantes en transferencias electrónicas de dinero, la Electronic Funds Transfer Act (EFT) protege tanto al consumidor como a las instituciones financieras. Asimismo, establece la necesidad de contar con un mecanismo capaz de proteger la integridad de los sistemas de transferencias electrónicas de dinero mediante el reporte de errores y la complementaria obligación del banco de examinar dichos errores e informar a los consumidores sobre el resultado de la investigación realizada.

En términos generales, podemos afirmar que la EFT se preocupa por la información financiera, tanto de los individuos como de las instituciones financieras mismas. Para ello la institución se verá obligada a facilitar a la institución que reciba la transferencia, información tal como la cantidad de dinero, el tipo de transferencia a ser realizada, la identidad de los consumidores involucrados en la transferencia y de cualquier tercera parte, y la localización de la terminal utilizada para realizar dicha transferencia (Congreso de los Estados Unidos de América, 1978).

### *Equal Credit Opportunity Act of 1974*

(Congreso de los Estados Unidos de América, 1974)

Relacionada fundamentalmente con datos crediticios, la Equal Credit Opportunity Act (ECOA) establece disposiciones tendientes a proteger a todo aplicante a cualquier tipo de operación crediticia frente a discriminación relacionada con su etnia, color de piel, religión, país de origen, estado marital, edad o al hecho de que este haya incoado un proceso de protección al consumidor de créditos.

Esta ley se relaciona con la protección de datos personales en dos frentes fundamentales, el primero de ellos en tanto hace mención a informaciones sensibles y al derecho de no discriminación del usuario. En segundo lugar, establece esta ley la obligación de las instituciones financieras de almacenar por un plazo no menor a un año, toda información relacionada con la extensión, renovación o continuación de un crédito (Mc Afee, Inc., 2013).

### *Fair and Accurate Credit Transactions Act of 2003*

(Congreso de los Estados Unidos de América, 2003)

Dirigida a luchar contra el robo de identidad de los consumidores y creada en el año 2003, la Fair and Accurate Credit Transactions Act (FACTA) establece disposiciones relativas a la precisión, privacidad, y límites de las transferencias de información crediticia, a la vez que fortaleció el derecho de acceso a la Información por parte de los interesados.

Las principales disposiciones de FACTA incluyen la necesidad de brindar reportes crediticios gratuitos a los consumidores estadounidenses (los cuales tradicionalmente debían ser comprados a compañías encargadas del manejo de tales datos[152]); la capacidad de los ciudadanos de alertar a las agencias crediticias sobre fraudes realizados en su contra; la necesidad de que estas compañías no envíen en sus comunicaciones los números completos de seguridad social de los individuos; y el

[152] Específicamente a las compañías estadounidenses Experian, TransUnion y Equifax, siendo especialmente necesario mencionar la conocida participación de esta última en la venta de información al gobierno estadounidense (ver Anexo 7).

derecho de los individuos afectados por robos de identidad de las transacciones realizadas por el impostor (Privacy Rights Clearinghouse, 2014).

### *FACTA Disposal Rule of 2005*

(Congreso de los Estados Unidos de América, 2005)

Dirigida a complementar las disposiciones de FACTA, esta ley impone a todo individuo o negocio que utilice información contenida en informes crediticios con fines de lucro la obligación de deshacerse de manera apropiada de dicha información. Esta ley establece medios específicos de destrucción de dicha información, como por ejemplo la quema, pulverización, o el despedazamiento de los documentos físicos que contengan dichos informes crediticios, y el borrado o destrucción de los medios digitales que cumplan la misma función.

### *Fair Credit Reporting Act of 1970*

(Congreso de los Estados Unidos de América, 1970)

Promulgada durante 1970, la Fair Credit Reporting Act (FCRA) regula la recolección, diseminación y uso de información de consumidores (incluyendo información crediticia de los consumidores) y forma parte del marco legal que fundamenta los derechos de los consumidores estadounidenses en materia crediticia.

Dirigida a proteger la información relacionada con la solvencia de un consumidor de crédito, su capacidad de crédito, su carácter y reputación, sus características personales y modo de vida, la FCRA posee un amplio ámbito de aplicación y establece

básicamente los siguientes derechos de los consumidores (Consumer Financial Protection Bureau, 2013):

- Derecho a ser informado si los datos crediticios de un consumidor han sido utilizados en su contra.
- Derecho a saber qué datos se encuentran en el expediente personal de cada consumidor.
- Derecho a solicitar un reporte crediticio.
- Derecho a oponerse a aquella información incompleta, inexacta o imposible de verificar y la obligación de las agencias crediticias de corregir o eliminar dicha información.
- Obligación de las agencias crediticias de no reportar información antigua (más de 7-10 años).
- Obligación de las agencias crediticias de asegurar que el acceso a la información crediticia sea limitado solamente a personas o entes legitimados por la FCRA.
- Obligación de las agencias crediticias de obtener el consentimiento del sujeto de datos previamente a liberar información crediticia a sus empleadores.
- Derecho de limitar las comunicaciones no deseadas relacionadas con la información crediticia del individuo.
- Derecho del consumidor de perseguir legalmente a quienes violen los derechos ya mencionados.

### *Fair Debt Collection Practices Act of 1996*

(Congreso de los Estados Unidos de América, 1978)

Dirigida a limitar las formas abusivas de recopilación de información relacionada con las deudas[153] de los consumidores, la Fair Debt Collection Practices Act (FDCPA) limita las acciones en las que pueden incurrir las agencias de cobro de deudas y establecen los derechos de los consumidores.

De esta manera, la FDCPA prohíbe específicamente a estas empresas el contactar a terceras partes ajenas a la deuda, el amenazar vanamente al deudor, el realizar llamadas repetitivas, en horas no adecuadas o a lugares inconvenientes (trabajo, por ejemplo), informar al patrón del deudor sobre el motivo de la llamada, el uso de lenguaje obsceno o discriminatorio, el envío de cartas que emulen el formato oficial de un juzgado, la persecución de cobros abusivos, amenazar al deudor con arresto policial de no pagar sus deudas, entre otros (Larson, 2011).

### *Family Education Rights and Privacy Act of 1974*

(Congreso de los Estados Unidos de América, 1974)

Vigente como ley federal estadounidense a partir del 21 de Agosto de 1974, la Family Education Rights and Privacy Act (FERPA) pretende la protección de la privacidad de los estudiantes al brindarles control sobre los registros existentes que se relacionen con su educación y que sean mantenidos por una institución o agencia educativa (o por una

[153] Definidas por esta ley como cualquier obligación que pese sobre un consumidor y que le imponga el pago de dineros a partir de una transacción en la cual dinero, propiedades, seguros o servicios sean utilizados primariamente para propósitos personales, familiares o del hogar.

tercera parte que actúe en nombre de alguna de las anteriores) que reciban sus fondos a partir del presupuesto del Departamento de Educación Estadounidense.

FERPA procura fundamentalmente proteger a los estudiantes matriculados en los cursos impartidos por las instituciones anteriormente mencionadas (independientemente de la modalidad en la cual el curso sea impartido), para lo cual instituye formalmente el derecho del estudiante de revisar su expediente académico y solicitar enmiendas a este en caso de considerar que incluye elementos inexactos o erróneos.

Por otro lado, contempla también la capacidad del estudiante de aceptar voluntariamente que el contenido de su registro académico sea publicado y de establecer quejas ante el Departamento de Educación por cualquier violación realizada por la institución académica a las disposiciones de FERPA (University of Virginia, 2013).

Finalmente, debe apuntarse que esta norma brinda a los estudiantes importantes herramientas para salvaguardar su privacidad. Sus disposiciones no solamente afectan a las instituciones educativas en la cuales se encuentre matriculado, sino también a las agencias estatales y federales, para las cuales establece maneras específicas en las cuales la información personal debe ser transferida.

### *Federal Trade Commission Act of 1938*

(Congreso de los Estados Unidos de América, 1938)

La Federal Trade Commision Act adquiere importancia para el sistema de protección a la privacidad estadounidense al crear la Comisión Federal de Comercio (FTC), la cual se

encarga de evitar competencia desleal, facilitar la compensación de los consumidores ante actos de comercio perjudiciales, establecer normativa especial en materia de comercio, investigar la organización, negocios, prácticas y administración de las entidades comerciales y recomendar al congreso propuestas legislativas apropiadas.

Gracias a este cúmulo de responsabilidades, y especialmente a su responsabilidad de investigación, la FTC posee una jurisdicción sumamente amplia que incluye a las más diversas empresas, por lo cual puede imponer sanciones a aquellas compañías que no cumplan con las estipulaciones de sus declaraciones de privacidad. Gracias a ello, la FTC vela por la protección de los más diversos tipos de datos personales, los cuales incluyen desde información general sobre el consumidor, hasta información obrero-patronal.

Finalmente, debe mencionarse que la FTC se encuentra legitimada tanto para iniciar procesos de oficio, como para establecer normativas generales que regirán industrias específicas, por lo cual se encuentra en capacidad de obligar a las empresas a cesar y desistir de prácticas comerciales capaces de generar afectaciones a los derechos o intereses de los consumidores.

### *Financial Services Regulatory Relief Act of 2006*

(Congreso de los Estados Unidos de América, 2006)

Creada para enmendar la FDCPA con miras a aumentar la productividad de las instituciones aseguradas de depósito en los Estados Unidos, la Financial Services Regulatory Relief Act (FSRRA) se relaciona con la protección de los datos personales en

tanto contempla, a lo largo de su título VII, la creación de formularios modelo de protección de datos personales acordes con las disposiciones del sistema de Safe Harbor de la Unión Europea (que se estudiará más adelante).

### *Gramm-Leach-Bliley Financial Modernization Act of 1999*

(Congreso de los Estados Unidos de América, 1999)

Creada en 1999 por el Congreso Estadounidense con miras a modernizar (desregular) los servicios financieros, la Gramm-Leach-Bliley Financial Modernization Act (GLBA), establece la obligación de suministrar a los consumidores de servicios financieros con información suficiente en materia de privacidad, como para explicarles a los interesados qué tipo de información recolectará la entidad financiera, con quiénes será compartida, de qué manera será utilizada y cómo será protegida.

Por otro lado, las disposiciones en materia de protección de datos financieros incluidas en esta ley establecen la necesidad de brindar al consumidor la posibilidad de evitar que dicha información sea compartida con terceras partes (McAfee, Inc., 2013), así como la obligación de las instituciones financieras de crear un plan de seguridad de la información en el cual se establezcan, como mínimo (Congreso de los Estados Unidos de América, 1999):

- Un encargado de administrar la seguridad de la información.
- La construcción de un análisis de riesgos completo para todos aquellos departamentos de la institución que manejen información sensible del interesado.

- La generación de un programa capaz de monitorear y probar la seguridad de la información.
- Adaptaciones a las medidas de seguridad de la información conforme cambien las maneras en que la información sea recolectada, almacenada y utilizada.

Finalmente, la ley establece la necesidad de las instituciones financieras de evitar los crímenes informáticos y robos de identidad realizados mediante ingeniería social, lo cual puede ser logrado de diversas maneras; entre las cuales se encuentra el reforzamiento del plan de seguridad de la información con programas de entrenamiento del personal de la institución para detectar dichas amenazas.

### *Health Insurance Portability Act of 1996*

(Congreso de los Estados Unidos de América, 1996)

Promulgada el 21 de agosto de 1996, la Health Insurance Portability Act (HIPAA) busca la protección de los trabajadores y sus familias cuando cambian o pierden sus trabajos, a la vez que establece provisiones de simplificación administrativa dentro de las cuales se encuentran el establecimiento de estándares nacionales para las transacciones electrónicas de datos médicos. Asimismo, esta ley se caracteriza por extender el ejercicio del derecho a la privacidad a los jóvenes de 12 a 18 años de edad, requiriendo su consentimiento previo a cualquier liberación de información médica a cualquier persona (incluyendo a los padres del menor) (U.S. Department of Health & Human Services, 2013).

En términos generales, se puede afirmar que HIPAA procura la protección de la privacidad de los individuos al obligar a todo proveedor de servicios de salud que transmita información médica por medios electrónicos, a proteger los registros y expedientes médicos de los interesados. Logra tal fin mediante la regulación de los usos válidos que pueden ser dados a los datos médicos (llamados "información médica protegida" por la ley) a la vez que regula los casos en los cuales dicha información puede ser liberada con o sin consentimiento del interesado.

De esta manera, HIPAA brinda al sujeto de datos los derechos de revisión, corrección y eliminación de su información médica, así como el derecho a solicitar que los proveedores de salud utilicen medios determinados para comunicarse con el interesado (evitando las llamadas telefónicas por ejemplo). Por otra parte, la norma establece sobre los proveedores obligaciones como el proteger la información a su disposición, el asegurar que toda transferencia sea realizada garantizando la confidencialidad de la información, el nombrar un oficial de privacidad y el notificar a los individuos sobre los usos dados a sus datos.

### *Health Information Technology for Economic and Clinical Health Act of 2009*

(Congreso de los Estados Unidos de América, 2009)

Dirigida a la promoción de las TICs en el establecimiento de infraestructura nacional de salud y la creación de expedientes electrónicos en el área de salud, la Health Information Technology for Economic and Clinical Health Act (HITECH) contiene también una serie de disposiciones relativas a la protección de datos médicos, que

resultarán aplicables a todas las entidades que se encontraban sujetas a las provisiones de HIPAA.

Específicamente, HITECH extiende la totalidad de las provisiones de HIPAA a los socios de negocios de las entidades de salud e incluye la obligación de los proveedores de servicios de salud de realizar notificaciones a los sujetos de datos, en caso de que se den violaciones a sus bases de datos o se vulnere de cualquier manera la seguridad de sus datos personales (IT Law Wiki, 2013). Finalmente, incluye también dentro de sus disposiciones reglas por seguir para liberar o compartir datos médicos dentro de un sistema de expedientes electrónicos[154].

### *Identity Theft and Assumption Deterrence Act of 1998*

(Congreso de los Estados Unidos de América, 1998)

Ley penal que criminaliza los robos de identidad, designando al individuo como víctima de este delito (anteriormente a su promulgación solamente eran considerados víctimas las compañías de crédito que sufrían desfalcos por causa de este delito). Esta ley establece sobre la FTC la responsabilidad de investigar las quejas contra las agencias de crédito y permite que la víctima pueda exigir una compensación por las afectaciones sufridas en caso de que el delincuente sea aprehendido y condenado (McAfee, Inc., 2013).

[154] Punto que ha sido objeto de debate en tanto recientes modificaciones en las políticas del Departamento de Salud estadounidense implicaron que los datos médicos de todo paciente que hubiera brindado su consentimiento general (según las disposiciones de HIPAA) ahora vería su información distribuida libremente entre más de 2 millones de proveedores de servicios de salud y sus socios comerciales (Institute for Health Freedom, 2010).

### *Privacy Act of 1974*

(Congreso de los Estados Unidos de América, 1974)

Creada como respuesta a la preocupación por el creciente uso de bases de datos por parte del gobierno federal estadounidense y las consecuencias que la compilación de los datos podrían implicar para los derechos de los individuos, la Privacy Act de 1974 establece el principal marco normativo en materia de protección de datos con el que cuentan los Estados Unidos de América en el ámbito federal.

Esta ley protege al individuo mediante cuatro disposiciones básicas, que son resumidas por el Electronic Privacy Information Center de la siguiente manera: *"Primero, requiere que las agencias gubernamentales muestren al individuo todos los registros mantenidos sobre él o ella. Segundo, requiere que las agencias sigan ciertos principios, llamados "prácticas justas de información", cuando recopilen y manejen datos personales. Tercero, establece restricciones en las maneras mediante las cuales las agencias pueden compartir la información de un individuo con otras personas y agencias. Y finalmente, permite que los individuos demanden al gobierno por violar sus disposiciones"* (Electronic Privacy Information Center, 2013).

La norma cubre dentro de su rango de aplicación únicamente a los ciudadanos estadounidenses y a los residentes permanentes. Asimismo, la ejecución obligatoria de sus disposiciones se encuentra limitada a algunas de las agencias federales del país, como por ejemplo las ramas del Poder Ejecutivo, las agencias militares, las agencias reguladoras y las corporaciones estatales[155]. Asimismo, esta ley es aplicable a los "sistemas de registro", los cuales son definidos como cualquier grupo de registros en

[155] Encontrándose excluidas las agencias de policiales y de investigación judicial, así como los gobiernos estatales y regionales, entre otras.

los que la información pueda ser recuperada del sistema a partir del nombre del individuo o mediante un identificador que le sea asignado a este (Congreso de los Estados Unidos de América, 1974).

En el texto normativo se encuentran algunos de los principios de la protección de datos, como los de acceso a la información, consentimiento del interesado, publicidad y seguridad de la información. En conformidad con dichos principios, la ley es enfática en su prohibición de las bases de datos secretas, para lo cual establece la obligación de informar a todos los interesados sobre su existencia y de asegurar que este será capaz de revisar y copiar su propio expediente. Igualmente, protege esta normativa los derechos del sujeto de datos de solicitar la rectificación de los errores encontrados y de apelar la decisión que le impida hacerlo; así como de ser informado por la agencia misma sobre los pasos que debe seguir para demandarla judicialmente cuando lo considere necesario.

Enumera la norma doce casos específicos[156] en los cuales las agencias federales podrán liberar la información sin el consentimiento del interesado, así como la obligación de

[156] "• Cuando la liberación es realizada en favor de un empleado de la agencia que usualmente mantiene el registro y lo requiere para el ejercicio de sus funciones;
• Cuando la liberación es realizada bajo las disposiciones de la Freedom of Information Act;
• Cuando la liberación se da para un "uso de rutina";
• Cuando la liberación sea realizada a la oficina de censos con motivo de la realización de un censo;
• Cuando la liberación sea para fines de investigación estadística y se libere sin información personalmente identificable;
• Cuando la liberación favorezca a la administración nacional de archivos y registros como un registro de valor histórico;
• Cuando se libere para cualquier jurisdicción gubernamental dentro o bajo el control de los Estados Unidos para actividades de investigación judicial;
• Cuando la liberación sea realizada bajo circunstancias apremiantes que afecten la seguridad o salud de alguna persona;
• Cuando la liberación es realizada en favor del Congreso de los Estados Unidos o en favor de cualquier comité o subcomité del Congreso;
• Cuando la liberación sea realizada al Contralor General de la Oficina General de Contabilidad;
• Cuando la liberación sea justificada por una orden judicial; y

las agencias de mantener registros detallados (por un plazo no menor a cinco años o por la vida de los registros involucrados) de las liberaciones realizadas. Asimismo, se requiere que las agencias mantengan dentro de sus bases de datos la menor cantidad de información "relevante y necesaria" que sea posible, y en caso de que la información pudiera tener efectos adversos para el interesado, dicha información deberá ser provista por el individuo mismo, quien deberá ser informado a cabalidad del contexto que envuelve a tal liberación y las consecuencias de no proveer tal información (Congreso de los Estados Unidos de América, 1974).

Finalmente, la ley establece límites al intercambio de datos entre las agencias federales (y no federales) y a la implementación de programas informáticos dirigidos a comparar bases de datos. Para ello, se prohíbe realizar dichas comparaciones entre agencias que no posean un acuerdo formal que detalle el propósito de dicho programa, la justificación de este y sus resultados estimados, la descripción de los registros por ser comparados, los procedimientos específicos por seguir en materia de seguridad de la información, valoraciones de precisión de las mediciones y una sección que permita al Contralor General acceder a los registros necesarios para valorar la aplicación del acuerdo (Electronic Privacy Information Center, 2013).

### *Privacy Protection Act of 1980*

(Congreso de los Estados Unidos de América, 1980)

• Cuando la liberación sea realizada en favor de una agencia de informe del consumidor bajo las disposiciones del artículo 3711 del título 31 del Código de los Estados Unidos" (Congreso de los Estados Unidos de América, 1974).

A pesar de su título, la Privacy Protection Act of 1980 no establece mayores disposiciones dirigidas a la protección de la privacidad de los ciudadanos estadounidenses. Relacionada en mayor medida con la libertad de prensa que con la privacidad, esta ley prohíbe a los oficiales gubernamentales el buscar o incautar aquellos documentos que se crea fueron ideados para ser diseminados públicamente[157].

Si bien esta norma no se relaciona directamente con el área de protección de datos personales, debe considerarse relevante su mención en tanto las tecnologías convergentes han permitido que potencialmente todo individuo se convierta en autor y diseminador de contenidos, los cuales pueden incluir datos personales suyos o de terceros.

### *Right to Financial Privacy Act*

(Congreso de los Estados Unidos de América, 1978)

Creada con miras a proteger los registros y expedientes financieros de los individuos ante potenciales pesquisas gubernamentales, la Right to Financial Privacy Act (RFPA) prohíbe la liberación de tales datos por parte de cualquier institución financiera sin el consentimiento expreso del titular de estos (McAfee, Inc., 2013).

### *Sarbanes-Oxley Act of 2002*

(Congreso de los Estados Unidos de América, 2002)

[157] Por lo que básicamente procura esta es norma proteger fundamentalmente la confidencialidad de las fuentes periodísticas.

Esta ley federal fue creada en el año 2002 con el fin de establecer estándares mayores en la gestión de compañías públicas con valores en el mercado mayores a los setenta y cinco millones de dólares. Dentro de los principales cambios requeridos por la Sarbanes-Oxley Act (SOX) en las prácticas financieras y la gobernanza corporativa de las empresas, es posible encontrar elementos relativos al mantenimiento de los registros corporativos.

Específicamente en el área de protección de datos, esta ley se preocupa tanto por los datos financieros, como por los demás datos que pudieran ser relevantes para una empresa pública. Es por ello que dicta buenas prácticas en materia de seguridad de la información, que incluyen reglas con respecto a la destrucción, alteración o falsificación de los registros, los períodos de retención de información y los tipos de información que debe ser resguardada en los registros de estas compañías (Orric, Herrington & Suitcliffe LLP, 2002).

### *Telecommunications Act of 1996*

(Congreso de los Estados Unidos de América, 1996)

Ideada como la primera transformación significativa de la legislación estadounidense en materia de telecomunicaciones, la Telecommunications Act incluye dentro de sus disposiciones una sección dirigida a la protección de la privacidad del consumidor, lo cual logra mediante el establecimiento de una regla general que obliga a todo operador de servicios de telecomunicaciones a proteger la confidencialidad y privacidad de la información de sus usuarios.

La Telecommunications Act contempla restricciones relevantes al acceso, uso y revelación de la información de los usuarios de servicios de telecomunicaciones; sin por ello dejar de lado la capacidad del proveedor de realizar cualquiera de estas acciones en caso de que sean necesarias para proveer el servicio, realizar cobros y brindar información de localización de la llamada en casos de emergencia.

### *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*

(Congreso de los Estados Unidos de América, 2001)

Quizá la más famosa de las leyes estadounidenses por ser estudiadas, la Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT) fue creada como respuesta a los ataques terroristas sufridos en dicho país el 11 de septiembre de 2001. Caracterizada tanto por incluir cambios significativos en el marco legal estadounidense, como por el hecho de haber sido aprobada por el Congreso estadounidense sin debates ni cambios, la ley modifica más de 12 leyes preexistentes.

La USA PATRIOT Act se preocupa por aumentar las capacidades de respuesta y prevención de las agencias de inteligencia e investigación judicial estadounidenses mediante la implementación de medidas como la autorización judicial para interceptar varios equipos o dispositivos de telecomunicaciones a la vez, la diseminación y transferencia de información de procesos de investigación judicial a través de las diversas agencias, la facilitación del acceso gubernamental a los archivos de negocios

privados, la disminución de los requisitos necesarios para interceptar comunicaciones realizadas en el extranjero (Abramson & Godoy, 2006).

Las implicaciones de la USA PATRIOT Act en materia de protección de datos son amplísimas. En tanto su contenido se refiere ampliamente a las medidas de vigilancia e intercepción de telecomunicaciones (y gracias a que es aplicada en la práctica a la vigilancia de las más diversas industrias relacionadas con el sector de TICs) es posible afirmar sin temor al equívoco, que las capacidades de intercepción y recopilación de datos que esta permite se ve solamente limitada por las capacidades técnicas de las agencias encargadas de realizar tales acciones.

Esta ley ha sido enmendada en diversas ocasiones con miras a incrementar su ámbito de aplicación y extender sus alcances temporales.

### *Video Privacy Protection Act of 1988*

(Congreso de los Estados Unidos de América, 1988)

Poco conocida dentro del contexto normativo federal estadounidense, la Video Privacy Protection Act (VPPA) es promulgada a partir de la liberación, en 1988, de los registros de alquiler de películas de una figura pública de la época. Se caracteriza por ser *"una de las más fuertes protecciones a la privacidad del consumidor frente una forma específica de recolección de datos"* (Electronic Privacy Information Center, 2013).

Originalmente, la VPPA establecía una prohibición general sobre la liberación de información personalmente identificable, salvo en caso de contar con consentimiento

del sujeto de datos, a la vez que obligaba a las tiendas de alquiler de videos a destruir los registros a más tardar un año de la finalización de su relación con el cliente.

A pesar de contar con tan ventajosas disposiciones, en la actualidad la VPPA se encuentra en el umbral de una enmienda[158] por medio de la cual se pretende eliminar la prohibición general y permitir que las compañías liberen la información de alquiler de películas con base en un consentimiento general del usuario.

### La Carta de Derechos de Privacidad del Consumidor y el Marco de Protección de la Privacidad y la Innovación en la Economía Global Digital

A principios del año 2012, la administración Obama hizo público un proyecto dirigido a realizar una reforma comprehensiva en el marco legal estadounidense en materia de privacidad del consumidor. Según la Casa Blanca, el proyecto se dirigía tanto a la creación de un marco básico de derechos del consumidor por ser adoptados por las compañías que manejan datos personales en los Estados Unidos, como a la creación de políticas corporativas afines a dicho marco de derechos.

El día de la presentación del proyecto, el mismo presidente Barack Obama anunció que este se basaba en reconocer que *"Los consumidores estadounidenses no pueden esperar más por reglas claras del camino que aseguren la seguridad de su información personal en línea (…) Conforme el Internet evoluciona, la confianza del consumidor se torna esencial para el continuo crecimiento de la economía digital. Es por ello que una carta de Derechos de*

[158] Impulsada específicamente por Netflix y otras compañías que ofrecen el servicio de alquiler de películas por medio del internet.

*Privacidad del Consumidor es tan importante. Para que los negocios tengan éxito en línea, los consumidores deben sentirse seguros. Siguiendo este proyecto, las compañías, los representantes de los consumidores y quienes crean las políticas pueden ayudar a proteger a los consumidores y asegurar que el Internet continúe siendo una plataforma para la innovación y el crecimiento económico"* (Office of the Press Secretary - The White House, 2012).

Constituyéndose como el primer esfuerzo por regular la manera en que las entidades privadas estadounidenses manejan los datos personales[159], el programa marco presentado por la administración Obama se compone de cuatro elementos básicos: la Consumer Privacy Bill of Rights (Carta de Derechos de Privacidad del Consumidor), el proceso de múltiples interesados para determinar cómo deberán ser aplicados los principios establecidos por la Carta de Derechos en los diversos contextos de negocios, un sistema de "ejecución efectiva", y un compromiso por incrementar la interoperabilidad con los sistemas de privacidad y protección de datos existentes en otros países (The White House, 2012).

Como primer punto de este programa, la Carta de Derechos de Privacidad del Consumidor establece un conjunto de principios de prácticas justas de información cuya implementación (tanto en códigos de conducta corporativos[160], como en las nuevas leyes creadas por el Congreso) será incentivada por la administración.

Básicamente, la carta establece los siguientes principios:

[159] El documento es enfático en aclarar que su ámbito de aplicación será limitado solamente al sector privado y que un conjunto distinto de disposiciones constitucionales y legales serán aplicables al acceso gubernamental a datos en posesión de los particulares.
[160] De conformidad con el modelo de auto regulación que ha sido implementado históricamente en Estados Unidos, los principios establecidos por esta iniciativa no buscan más que definir puntos cuya implementación queda a discreción de las compañías.

- *"Control individual: Los consumidores tienen el derecho a ejercer el control sobre qué datos personales son recopilados por las compañías y como serán utilizados.*
- *Transparencia: los consumidores tienen el derecho de contar con información fácilmente comprensible y accesible sobre las prácticas de privacidad y seguridad.*
- *Respeto por el contexto: los consumidores tienen el derecho de esperar que las compañías recojan, usen y revelen los datos de maneras consistentes con el contexto en el cual los consumidores proveen los datos.*
- *Seguridad: los consumidores tienen el derecho a un manejo seguro y responsable de sus datos personales.*
- *Acceso y precisión: los consumidores tienen el derecho de accesar y corregir los datos personales en formatos utilizables, de maneras apropiadas con la sensibilidad de los datos y el riesgo de consecuencias adversas a los consumidores si los datos son inexactos.*
- *Recolección enfocada: los consumidores tienen derecho a límites razonables sobre los datos personales que pueden ser recogidos y conservados por las empresas.*
- *Responsabilidad: los consumidores tienen el derecho de que sus datos personales sean manejados por compañías que cuenten con las medidas apropiadas para asegurar que se adhieren a la Carta de Derechos de Privacidad del Consumidor "* (The White House, 2012, pág. 1).

El segundo punto del programa versa sobre el fomento de procesos de múltiples interesados[161] dirigidos a la creación de códigos de conducta vinculantes para las compañías. Dichos procesos buscarán formar acuerdos vinculantes[162] entre las partes

[161] Actualmente se encuentra en marcha el primero de estos procesos de múltiples interesados, el cual ha sido adoptado por la National Telecommunications & Information Administration y se dirige a la *"creación de un código de conducta para brindar transparencia sobre cómo las compañías que proveen aplicaciones y servicios interactivos para dispositivos móviles manejan datos personales"* (National Telecommunications & Information Administration, 2013).

[162] Cuya adopción quedará supeditada a una decisión final tomada por las empresas y tras esta las empresas se verán obligadas a cumplir con el código de conducta aprobado.

que sostienen intereses en las diversas áreas de la privacidad y la protección de datos personales mediante foros abiertos, transparentes y de participación voluntaria, en los cuales la administración fomentará la participación pública.

En tercer lugar, el gobierno estadounidense busca incrementar las potestades de la Federal Trade Commission al fortalecer sus capacidades de investigación, intervención y sanción en caso de que una compañía no cumpla con sus compromisos en materia de privacidad. Asimismo, se prevé dentro del modelo el fortalecer legislativamente a al FTC con miras a autorizarla a vigilar la aplicación de la Carta de Derechos de Privacidad del Consumidor.

Como punto final, la carta reconoce el carácter intrínsecamente transfronterizo del internet, por lo que busca fomentar la interoperabilidad legal en materia de privacidad y protección de datos. Dicha interoperabilidad busca fundamentalmente el reconocimiento mutuo de los sistemas de protección de datos existentes en el orbe y la cooperación en la aplicación de dichos sistemas.

Debe concluirse este apartado reconociendo el carácter innovador que poseen tanto la Carta de Derechos de Privacidad del Consumidor, como el programa marco que la circunscribe. Dentro de un sistema legal como el estadounidense (marcado tradicionalmente por la auto regulación del mercado), esta iniciativa se constituye como un primer reconocimiento a la necesidad de estandarizar los principios de protección de datos entre las compañías y a la vez plantea algunas interesantes ideas que tal vez pudieran ser aplicadas en nuestro país.

### *Síntesis de la Primera Sección*

Modelo Europeo de Protección de Datos Personales

*A lo largo del cual es estudiado el marco legal fundamental vigente en Europa en materia de protección de datos personales, con énfasis especial en analizar las directivas, regulaciones y las propuestas de reforma planteadas a la fecha.*

- Europa no es solamente la cuna de la protección de datos moderna, sino que posee en la actualidad el sistema más complejo y completo de protección de datos en el ámbito mundial, caracterizado por sus altos estándares y la gran seriedad con que es tratado el tema por parte de los entes reguladores nacionales e internacionales.
- La protección brindada en Europa se encuentra enmarcada por el siguiente marco legal fundamental:
    - Carta de los Derechos Fundamentales de la Unión Europea: La cual reconoce expresamente la protección de datos personales como un derecho fundamental que se torna de adopción vinculante en el ámbito europeo.
    - Tratado de la Unión Europea: Pilar fundamental en el funcionamiento de la Unión, establece los parámetros generales fundamentales aplicables a todos los países miembros, compromete a los países a adoptar disposiciones sobre derechos fundamentales y se refiere al sistema de seguridad común europeo (límite a la protección de datos).
    - Tratado sobre el Funcionamiento de la Unión Europea: Reconoce expresamente el derecho a la protección de datos personales y eleva ante el Parlamento Europeo y el Consejo la creación de las normas regionales sobre el tema.
    - Convenio 108 del Consejo de Europa: Único instrumento internacional jurídicamente vinculante con potencial para ser aplicado globalmente; define una serie de principios fundamentales reconocidos universalmente y establece normas tecnológicamente neutras, adaptables a los marcos legales internacionales y aplicables en niveles público y privado.

  - Protocolo adicional al Convenio 108 del Consejo de Europa: Procura mejorar la aplicación de los principios del Convenio mediante provisiones vinculantes necesarias frente al progreso tecnológico y el intercambio de datos personales en los mercados globalizados.

- En el ámbito europeo, la materia se ha visto delimitada por una serie de Directivas que establecen un marco por seguir por parte de los países de la región, a saber:
  - Directiva 95/46/EC: Dirigida al establecimiento de un marco único para la región, requiere a los países europeos la creación de leyes comprensivas de protección de datos siguiendo los estándares mínimos por ella establecidos.
  - Directiva 2002/58/EC: Establece los fundamentos regulatorios para el procesamiento de datos en los servicios de comunicación, instituyendo disposiciones en materia de seguridad del procesamiento, retención de datos, comunicaciones no solicitadas, las cookies, los directorios públicos y el establecimiento de controles gubernamentales.
  - Directiva 2006/24/EC: Referida a la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas, adopta una posición excesivamente permisiva respecto a dichas actividades, por lo que fue invalidada el 8 de abril de 2014 por la Corte Europea de Justicia.
  - Decisión Marco 2008/977/JHA: Procura la protección de los derechos de las personas físicas frente a las actividades políticas y judiciales en materia penal, para lo cual establece reglas básicas de protección a los derechos y libertades fundamentales, y específicamente a los datos personales.
  - Directiva 2009/136/EC: Refuerza la Directiva 2002/58/EC al redoblar las disposiciones relativas al consentimiento informado necesario para la instalación de cookies en los equipos de los usuarios.
- La Unión Europea cuenta también con las disposiciones de la Regulación 45/2001, la cual establece la Autoridad Europea de Protección de Datos y procura el aseguramiento de un alto nivel de protección en un marco nacional y regional que asegure el cumplimiento de los principios básicos de la protección de datos.

- Finalmente, la Unión cuenta con dos proyectos de reforma dignos de mención en tanto pretenden cambios substanciales al sistema europeo de protección de datos, dirigidos a su actualización y a asegurar una mayor protección al usuario en áreas como la policial y judicial (las cuales hasta el momento cuentan con un mínimo de protección); las reformas en cuestión son las siguientes:
    - Propuesta de Reglamento General de la Protección de Datos: Realiza una relectura de la protección de datos existente en la Directiva 95/46/EC con miras a su actualización y mejoramiento, incorporando disposiciones necesarias para asegurar una mayor aplicación de la protección de datos en el contexto actual de la Unión.
    - Propuesta de Directiva del Parlamento Europeo y del Consejo: Especialmente enfocada en el área de la cooperación policial y judicial en asuntos criminales, procura eliminar los vacíos existentes en la Decisión Marco 2008/97/JHA.

Modelo Estadounidense

*A lo largo de la cual es estudiada la legislación federal estadounidense relevante al tema de la privacidad y la protección de datos, con miras a determinar la extensión de la protección brindada en un este sistema en contraposición con el europeo.*

- Dada su percepción distinta de la privacidad respecto a la existente en los países de tradición civilista, el sistema estadounidense ha sido caracterizado como "diametralmente opuesto al sistema europeo" (Guadamuz, 2000), en el cual se ha evitado por lo general la regulación de las políticas de privacidad y protección de datos, y en su lugar se ha optado por fomentar un modelo de auto-regulación (o regulación mínima).
- El sistema estadounidense deja a disposición de las empresas y de los consumidores la toma de decisiones en materia de protección de datos y procura evitar la intervención estatal, en donde esta no sea absolutamente necesaria. A pesar de tal situación, el marco legislativo federal de dicho país cuenta con una buena cantidad de leyes relevantes al tema, a saber:
    - Americans with Disabilities Act: relativa a la protección de datos medicos.

- Bank Secrecy Act: relacionada con la protección de datos financieros (información transaccional).
- Cable Communications Privacy Act: la cual asegura el derecho de acceso a la información y protege los datos de subscripción.
- Children's Internet Protection Act: que procura la protección de los datos de personas menores de edad.
- Children's Online Privacy Protection Act: que amplía la protección de los datos de personas menores de edad al Internet.
- Computer Fraud and Abuse Act: que castiga los ataques a los sistemas informáticos y protege la información financiera, estatal o privada.
- Communications Assistance for Law Enforcement Act: facilita las escuchas telefónicas obligando a los operadores a rediseñar la arquitectura de sus redes de telecomunicaciones.
- Computer Marching and Privacy Protection Act: busca proteger a los administrados frente a la recopilación, intercambio, procesamiento y comparación de sus datos por parte de las agencias estatales.
- Consumer Credit Reporting Reform Act: relativa a la protección de los datos de crédito.
- Drivers Privacy Protection Act: prohíbe la comunicación o revelación de los datos personales relacionados con los registros de vehículos y de informaciones "altamente restringidas" (imagen, número de seguridad social e información médica).
- Electronic Communications Privacy Act: establece provisiones sobre el acceso, uso, revelación, interpretación y protección de la privacidad de las comunicaciones electrónicas (pero no ha sido actualizada en más de 25 años, lo cual la inutiliza).
- Electronic Freedom of Information Act: procura garantizar el derecho al acceso a la información pública y a toda información gubernamental que verse sobre individuos.
- Electronic Funds Transfer Act: la cual se preocupa sobre la información financiera, tanto individual como institucional.

- Equal Credit Opportunity Act: que protege los datos crediticios frente a discrimación, menciona la información sensible y se establece disposiciones sobre retención de datos.
- Fair and Accurate Credit Transactions Act: establece disposiciones relativas a la presición, privacidad y límites de las transferencias de información crediticia y al acceso a la información por los interesados.
- FACTA Disposal Rule: complementa la ley anterior y establece el deber de destruir la información que ya no sea necesaria.
- Fair Credit Reporting Act: posee un amplio ámbito de aplicación y asegura una importante serie de derechos a los consumidores relacionados con sus datos personales (fundamentalmente crediticios).
- Fair Debt Collection Practices Act: limita las formas de recopilación de información relativa a deudas del interesado.
- Family Education Rights and Privacy Act: protege la información académica de los estudiantes, a la vez que les reconoce un número de derechos frente a instituciones educativas y agencias estatales o federales.
- Federal Trade Commission Act: crea la Comisión Federal de Comercio, encargada de velar por la protección de los datos personales en el país.
- Financial Services Regulatory Relief Act: contempla la creación de formularios de protección de datos acordes con el programa de Safe Harbor de la Unión Europea.
- Gramm-Leach-Bliley Financial Modernization Act: obliga a las instituciones financieras a suministrar información suficiente en material de privacidad a los consumidores y a crear un plan de seguridad de la información.
- Health Insurance Portability Act: establece estándares nacionales para las transacciones electrónicas de datos medicos y extiende el derecho a la privacidad a los jóvenes de 12 a 18 años de edad (requiriendo su consentimiento previo a cualquier liberación de datos).
- Health Information Technology for Economic and Clinical Health Act: contiene provisiones en relación con la protección de datos médicos en relación con la notificación en caso de violación a sus datos y define los

pasos necesarios para liberar o compartir datos médicos dentro de un sistema de expedientes electrónicos.

- Identity Theft and Assumption Deterrence Act: criminaliza los robos de identidad e impone a la FTC la responsabilidad de investigar las quejas contra las agencias de crédito.
- Privacy Act: establece el principal marco normativo federal en material de privacidad y protección de datos, asegurando a los ciudadanos y residentes estadounidenses el acceso a la información en bases de datos gubernamentales, exigiendo el seguimiento de prácticas justas de información, restringe el intercambio de información y permite a los individuos demandar al gobierno en caso de incumplir sus disposiciones.
- Privacy Protection Act: relacionada en mayor medida con la libertad de prensa que con la privacidad, prohíbe que oficiales gubernamentales incauten documentos ideados para su diseminación pública.
- Right to Financial Privacy Act: prohíbe la diseminación de datos financieros sin el consentimiento expreso del titular.
- Sarbanes-Oxley Act: dicta buenas prácticas de seguridad de la información atinentes a los datos financieros de los consumidores.
- Telecommunications Act: contempla restricciones en material de acceso, uso y revelación de la información de los usuarios de servicios de telecomunicaciones.
- Uniting and Strenghtening America by Providing Appropiate Tools Requiered to Intercept and Obstruct Terrorism Act: aumenta las capacidades de retención, intercepción, diseminación, transferencia y acceso de datos por parte de las agencias de seguridad nacional estadounidense en el ámbito nacional y en el extranjero.
- Video Privacy Protection Act: establece una prohibición general sobre la liberación de información personalmente identificable (salvo que se cuente con consentimiento informado). Esta prohibición probablemente será eliminada en los próximos años por una enmienda ya planteada.

- En el ámbito federal también se cuenta con la carta de derechos de privacidad del consumidor y el marco de protección de la privacidad y la innovación en la economía global digital, planteados con miras a la creación de un marco estandarizado de derechos del consumidor por ser replicados por las compañías en sus esfuerzos de autorregulación.

## Sección II: Modelos Nacionales

A lo largo de esta segunda sección se estudiarán otros dos modelos de protección de datos personales: el modelo de habeas data, (basado en el reconocimiento constitucional de este mecanismo procesal), y el modelo de protección de datos basado en el uso de instrumentos legales.

En el estudio del modelo basado en el habeas data, se enfocará la atención en el análisis de cinco países sudamericanos con miras a comprender la historia del desarrollo de este mecanismo procesal y la influencia que este causó en la región.

En segundo lugar, se examinarán también los ejemplos de cinco países que han adoptado leyes dirigidas a la protección de datos, para lo cual se elegirán países cuyos esfuerzos normativos permitan observar ejemplos de los diferentes niveles de protección que pueden ser obtenidos por medio de la protección legal.

### *Sistemas Legales Nacionales Basados en el Habeas Data*

Tal como se mencionara mencionamos ya a lo largo del capítulo segundo, la presente investigación asume dentro de sus postulados la diferencia terminológica que distingue los términos *autodeterminación informativa*, *habeas data* y *protección de datos personales*. Con base en ella puede afirmarse ya que el término *autodeterminación informativa* hace referencia a un derecho humano; mientras que se entenderá como *protección de datos personales* a un conjunto de técnicas y herramientas jurídico-informáticas dirigidas a materializar la autodeterminación informativa. Finalmente, debe recordarse que al hablar de *habeas data* se hace necesariamente referencia a una garantía procesal (o una acción constitucional) adoptada fundamentalmente dentro del ámbito constitucional de una buena cantidad de países latinoamericanos.

Según Guadamuz, *"Las acciones individuales ante una Corte Constitucional tienen una larga tradición en la historia del Derecho. La primera acción que existió, y probablemente la más famosa, es el Habeas Corpus (que se traduce bruscamente como "Debes tener el cuerpo"[163]). (…) Algunas otras acciones individuales existen, tales como el writ of mandamus (USA), amparo (España y México), Respondeat superior (Taiwan), etc. El más nuevo de estos mecanismos legales es el Habeas Data" (Guadamuz, 2000).*

[163] N.del T.: Se presenta aquí la traducción textual (inglés-español) del artículo de Guadamuz. La frase original latina correspondiente a esta figura es "*hábeās corpus ad subiiciendum"* la cual puede ser traducida como "que tengas tu cuerpo para exponer" o como "tendrás tu cuerpo libre" siendo hábeās la segunda persona singular del presente de subjuntivo del verbo latino habēre ('tener'), proveniente de la frase latina utilizada tradicionalmente para dar inicio al auto de comparecencia. Traducido por el Autor.

Dentro de los modelos de protección a la autodeterminación informativa existentes en el mundo, el modelo constitucional basado en el habeas data es representativo de los países sudamericanos. Tal situación responde básicamente a un proceso político, histórico y social que culminó en los años ochenta con la redacción o enmienda de gran cantidad de las constituciones políticas de los países de la zona, los cuales adoptaron y "tropicalizaron" dentro de sus nuevos textos fundamentales un derecho que, para la fecha, se encontraba en boga en Europa: el derecho de autodeterminación informativa (Martínez-Herrera, 2011, pág. 2).

Las palabras latinas "*habeas data"* pueden ser traducidas al español como "tener datos presentes", y tal como se mencionara anteriormente, responden a la acción constitucional que permitirá al individuo solicitar acceso a bases de datos, públicas o privadas, y, dependiendo de la jurisdicción aplicable, ejercer sus derechos de rectificación, actualización, eliminación y olvido. A pesar de ello, ha sido criticado usualmente por tratarse de un mecanismo de protección de carácter principalmente reparador, que no es ejercido por los interesados sino hasta la etapa de *output* del procesamiento de los datos (en el momento en que se ven afectados por estos).

En América Latina, el habeas data fue implementado de manera muy temprana por Brasil, país que lo hizo desde el año de 1992. Este ejemplo fue posteriormente seguido por Perú (1993), Argentina (1994) Ecuador (1996) y Colombia (1997), pero a pesar de tal situación, esta primera ola de países apegados al habeas data se caracterizaron por compartir una falla fundamental al establecer esta garantía procesal sin establecer al mismo tiempo los mecanismos procesales, judiciales y materiales necesarios para hacerlos efectivos. Tal como se verá a continuación, en los últimos años se ha

presentado una tendencia en la región dirigida hacia la solución de tales vacíos por medio de la promulgación de legislación especial para ello.

A continuación se estudiarán con mayor detenimiento cinco de los países que actualmente siguen el modelo de habeas data en alguna de sus modalidades: Brasil, Paraguay, Perú, Argentina y Colombia.

## Brasil

Brasil puede ser caracterizado como un país pionero al haber sido el primero en introducir el habeas data dentro de su sistema constitucional. El origen de dicha adopción es explicado por de Abreau Dallari, quien afirma que *"el Hábeas data llegó a Brasil a través de la Constitución de Portugal. Portugal hizo una constitución en 1976, después de una revolución que puso término a cuarenta años de dictadura. Y esta Constitución Portuguesa fue fuertemente influenciada por los pactos de derechos humanos. Pasó algo muy curioso: cuando Brasil consiguió cerrar el período de más de veinte años de dictaduras militares, fue a buscar en Portugal el modelo de constitución. Es muy fuerte la influencia de la Constitución Portuguesa en la Constitución de Brasil de 1988. Evidentemente hay peculiaridades, que derivan de condiciones que son típicas y específicas de Brasil, pero sin duda hay una influencia de este Constitución. Y el Hábeas data, [sic] está en la Constitución de Portugal, de este modo llegó a Brasil"* (De Abreau Dallari, 1997).

Según el autor supracitado, Brasil adopta el derecho de autodeterminación informativa (en la modalidad autóctona del habeas data) imitando a Portugal, país con quien compartía en la época elementos como la existencia de una policía política, tradicional,

violenta y arbitraria que poseía la costumbre de realizar registros de información respecto de aquellos individuos considerados enemigos del gobierno. En el marco de la reforma constitucional, el pueblo brasileño exigía tener acceso a dichos registros, y es por ello que finalmente es adoptado el habeas data en dicho país.

Gracias a tales fundamentos, la Constitución Política de la República Federativa del Brasil incluyó en su artículo 5 dos incisos (33 y 72) que conforman el actual habeas data en dicho país. El primero de estos incisos, el número 33, crea el derecho a la información al establecer que *"todos tienen derecho de recibir de órganos públicos, informaciones de su interés particular o de interés colectivo general" (De Abreau Dallari, 1997)*, mientras que el inciso 72 establece que "*Se concederá "habeas data": a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo;*" (Ministerio del Interior de la República Federativa del Brasil, 1988).

La adopción del habeas data en Brasil fue una medida totalmente innovadora para su época en tanto planteaba una solución diferente a sus antecesoras europeas, y brindaba un nuevo derecho legal que ofrecía *"un nuevo tipo de defensa de la privacidad diferente a los tipos Norteamericano y Europeo de Protección de Datos" (Guadamuz, 2000)*. Dicha solución fue posteriormente complementada por la ley Nº 9.507 del 12/11/1997, la cual establecía el reglamento al proceso de habeas data.

Dicha ley puede caracterizarse por establecer un sistema relativamente complicado en el cual el tribunal ante el cual debe presentarse la acción de habeas data cambiará según la identidad del imputado. Asimismo, incluye el derecho del sujeto de datos de

solicitar la inclusión de una anotación a los datos, en la cual se manifieste que estos están siendo actualmente disputados judicialmente (Guadamuz, 2000).

Más allá del texto constitucional y la ley supracitada, actualmente la República Federativa del Brasil no cuenta con una ley específica sobre la protección de datos ni con un ente regulador especializado en el tema, por lo que las disputas existentes deben ser usualmente ser discutidas con base en textos legales, tales como el Código Civil (artículos 12 y 21), el Código de Protección al Consumidor (artículos 43 y 46) y, en lo aplicable, las disposiciones de leyes referidas específicamente al sector gubernamental *(Ley 12,527/2011),* el sector fiscal (*Ley 5,172/1966)* y financiero *(Ley* 105/2001) (Goyanes, Porangaba, & Henrique, 2012).

Dicho marco legal permite dilucidar algunos otros elementos relevantes a la protección de datos personales. En cuanto a los derechos otorgados a los sujetos de datos, por ejemplo, el Código de Protección al Consumidor complementa los derechos constitucionales estableciendo en su artículo 43 inciso 2, que todo consumidor debe ser notificado por escrito cuando un archivo, registro o base de dato contenga datos personales relativos a su persona. Asimismo, este mismo código establece en su artículo 43 derechos equiparables al derecho al olvido permitiendo al consumidor requerir la eliminación de los datos negativos referidos a su persona que cuenten con más de cinco años de antigüedad.

Por otro lado, es posible afirmar que la legislación vigente en dicho país es aplicable a todo individuo y entidad legal, así como a los consumidores en su relación con sus proveedores de servicio, por lo que sus disposiciones serán aplicables tanto a los

operadores de redes de telecomunicaciones como a los diversos sitios web que manejen datos personales de usuarios (considerados usualmente consumidores por la jurisprudencia brasilera)[164].

A la fecha Brasil no cuenta con disposiciones específicas que impliquen excepciones a la legislación aplicable en materia de protección de datos personales. Iguales vacíos regulatorios existen en materia de notificación o registro de los procesadores de datos; obligaciones de los controladores de datos; reglas para tipos especiales de datos personales; cookies; privacidad en dispositivos móviles; procesamiento por terceras partes; transferencias internacionales de datos personales; ni disposiciones relativas a acuerdos modelo sobre transferencia de datos (o cualquier otro tipo de contrato modelo regulado legalmente en la materia) (Goyanes, Porangaba, & Henrique, 2012).

De conformidad con los elementos observados, es posible afirmar que en la actualidad Brasil cuenta con un sistema aún incompleto de protección de datos personales. Dicho sistema se basa fundamentalmente en elementos reparadores facilitados por el habeas data constitucional y las diversas leyes relacionadas con el tema para regular indirectamente esta materia, y pese a existir diversos proyectos legislativos tendientes a renovar el sistema de protección de datos brasileño, ninguno posee fecha cierta de entrada en vigencia.

Si bien por motivos de espacio no es posible en este momento detenerse a analizar la totalidad de los proyectos de ley relativos a la protección de datos que se encuentran actualmente en discusión en Brasil, a juicio del suscrito autor de esta investigación es

[164] Ver Alexandre Magno Silva Marangon v Google Brasil Internet Ltda (Tribunal Superior de Justicia de Brasil, 2010).

necesario mencionar el proyecto titulado "Marco Civil da Internet" (Poder Ejecutivo de la República Federativa del Brasil, 2011), el cual resalta por su excepcional naturaleza y origen.

Conocido usualmente en el ámbito internacional como la "Constitución del Internet" brasileña, el Marco Civil de Internet es un proyecto de ley generado a partir de la alianza que a lo largo del 2009 mantuvieron el Ministerio de Justicia de Brasil y el Centro para la Tecnologia y Socidad de la facultad de Derecho de la Fundação Getulio Vargas. Dirigida fundamentalmente al fomento de inclusión ciudadana en procesos colaborativos dirigidos a la creación del Marco Civil, dicha alianza permitió la formación de un proyecto de ley[165] que finalmente fue aprobado por el Ejecutivo para su discusión ante el Congreso Brasileño.

Basado fundamentalmente en ideales de libertad de expresión, neutralidad de la red, y de protección a la intimidad de los usuarios y de sus datos personales en internet, el Marco Civil da Internet plantea elementos tendientes a limitar la afectación al individuo, como por ejemplo la prohibición del monitoreo, filtro o revisión del contenido de los paquetes de datos enviados por los usuarios en su tránsito por el Internet[166] (Mari, 2013).

[165] El proceso colaborativo que llevó a la formulación del Marco Civil de Internet ha sido elogiado por muchos de los defensores del modelo de múltiples interesados en tanto se caracterizó por su transparencia y apertura en la generación de propuestas legislativas válidas para temas tan debatidos como la protección de datos, la neutralidad de la red y demás elementos relevantes a la gobernanza del internet (Maciel, Souza, & Affonso, 2011).

[166] Tema especialmente relevante en cara a los ya mencionados escándalos surgidos a lo largo del 2013 por el espionaje electrónico masivo en el cual incurrió el Gobierno de los Estados Unidos. Tras los cuales surgieron incluso propuestas que pretenden elevar el nivel de protección a los datos personales de los usuarios a niveles anteriormente inesperados (pretendiéndose por ejemplo la obligación de los proveedores de servicios de Internet el almacenar la totalidad de los datos personales dentro del país Sobre el tema, ver (Mari, 2013).

El proyecto del Marco Civil da Internet presenta excelentes perspectivas para complementar el sistema de habeas data vigente en la actualidad en Brasil. En muchos sentidos el proyecto se ha constituido como un ejemplo por seguir en tanto ha permitido la participación multisectorial en la formación de una propuesta legislativa viable, con respecto a la regulación de un tema tan amplio y complejo. Lastimosamente, en tanto aún se encuentra en discusión, son muy reales los peligros que amenazan el proyecto y su viabilidad real con respecto a la protección de datos y el habeas data, quedará aún por verse.

Debe resaltarse que el 25 de marzo de 2013 la Cámara de Diputados brasileña aprobó un texto sustitutivo (Congreso Nacional Brasileño, 2014) del proyecto del Marco Civil da Internet, caracterizado por superar las disposiciones de su antecesor en materia de retención de datos personales, neutralidad de la red, responsabilidad de los intermediarios, privacidad y los derechos y principios que procura establecer para todos los usuarios Brasileños de Internet (Moncau, Luiz Fernando; Nicoletti Mizukami, Pedro, 2014). Este texto sustitutivo fue finalmente aprobado como ley por parte del Congreso y firmado por la Presidenta Dima Rousseff el 23 de Abril de 2014.

### Paraguay

Siguiendo el ejemplo de Brasil, la Constitución Política de 1992 de la República del Paraguay establece expresamente el habeas data dentro de su artículo 135, el cual establece que *"Toda persona puede acceder a la información y a los datos que sobre sí*

*misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos"* (Convención Nacional Constituyente de Paraguay, 1992).

Tal como se puede observar, el texto constitucional paraguayo no solamente copia el brasileño sino que lo amplía, adoptando una mejor definición del habeas data y ampliando la tutela de este al proteger "*además de derechos personalísimos (privacidad, no discriminación) y no patrimoniales (convicciones religiosas, ideas políticas, etcétera); áreas de tipo patrimonial, ya que se lo plantea, también para atacar información equivocada sobre los bienes de un individuo o corporación*" (Sagüés, 1998).

Según Ramírez Salinas el artículo constitucional supra mencionado se encuentra basado en los siguientes presupuestos: *"1) la persona sólo puede conocer datos o informaciones sobre ella misma o sobre sus bienes, como así también, el uso y la finalidad de los mismos; 2) la información a la cual se quiere acceder debe constar en registros oficiales o privados de carácter público; 3) debe conocer en el hábeas data el magistrado competente; 4) la finalidad del hábeas data es la actualización, rectificación o destrucción"* (Ramírez Salinas, 2003, pág. 20).

Por su parte, Riascos Gómez señala que en el caso paraguayo la acción de habeas data implica una garantía constitucional específica (un amparo constitucional informativo que incluye la información y los datos personales) que en la práctica debe ser reclamada por medio del amparo genérico por cualquier persona con un interés general, colectivo o particular. Asimismo, los derechos que este otorga implican no

solamente el acceso y conocimiento a la información o datos de la persona, sino también a la finalidad y uso dados a estos. (Riascos Gomez, 2009).

Este conjunto de características hacen que en el caso paraguayo el habeas data se constituya como un proceso más simple que en el caso Brasileño. Específicamente, desde el punto de vista procesal la mención (y aplicación en la práctica) de un magistrado competente, ha terminado por simplificar el proceso al asignarse tal competencia al Juez de Primera Instancia en lo Civil y Comercial de Turno (Ramírez Salinas, 2003, pág. 20), a diferencia del caso Brasileño, con su multiplicidad de tribunales competentes.

Más allá del ámbito constitucional sin embargo, el panorama de la protección de datos personales en Paraguay no resulta tan favorable. El país cuenta a la fecha únicamente con dos leyes relacionadas con el tema (Leyes Nº 1682/01 y 1969/02) las cuales establecen disposiciones mínimas y especialmente relacionadas con la información financiera.

De conformidad con las anteriores leyes no puede ser liberada la información clasificada explícitamente como sensible (raza, etnia, preferencias políticas, salud, creencias religiosas o filosóficas, preferencia sexual, datos que puedan conducir a discriminación e imágenes de las personas o sus familias), mas sí podrá ser liberada toda la información no sensible (tal como nombre, número de identidad, domicilio, edad, estado civil, entre otros) de contarse con el consentimiento del interesado.

Aparte de estas disposiciones el marco legislativo paraguayo no cuenta con mayores procedimientos dirigidos a regular la acumulación, retención y liberación de los datos

personales (no se establece un ente regulador administrativo, por lo que las disputas deben ser solucionadas por vía civil o comercial), y con excepción de las pocas disposiciones penales existentes en el código penal del país la materia se encuentra aún sin ser regulada debidamente (Privacy International, 2012).

## Perú

En Perú se encuentra otro ejemplo de un país cuyo Derecho Constitucional ha adoptado el habeas data y en general la protección de los derechos fundamentales de sus ciudadanos. Los fundamentos de la protección de la intimidad de sus habitantes y del derecho a la autodeterminación informativa se encuentran en este país dentro de su Constitución Política, la cual establece desde su primer artículo que *"la protección de la persona y el respeto por su dignidad son el fin supremo de la sociedad y el Estado"* (Congreso Constituyente Democrático del Perú, 1993).

Dicha protección es ampliada por el artículo segundo de la Constitución Política del Perú, el cual establece los derechos fundamentales correspondientes a toda persona. Específicamente, dicho artículo establece en sus incisos 5 el derecho *"A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. (…)"* Y en su inciso 6 el derecho *"A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar"* (Congreso Constituyente Democrático del Perú, 1993).

El habeas data se encuentra establecido en Perú por el artículo 200 inciso 3 de su Constitución Política, la cual establece que *"Son garantías constitucionales: (…) 3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona que vulnera o amenaza los derechos a que se refiere el artículo 2º, incisos 5) y 6) de la Constitución"* (Congreso Constituyente Democrático del Perú, 1993). Estas disposiciones son complementadas por el artículo 202 inciso 2, en el cual se atribuye *"al Tribunal Constitucional: (…) 2. Conocer, en última y definitiva instancia, las resoluciones denegatorias de hábeas corpus, amparo, hábeas data y acción de cumplimiento"* (Congreso Constituyente Democrático del Perú, 1993).

Esta garantía constitucional es regulada en Perú por el Código Procesal Constitucional, el cual establece a lo largo de su título primero las disposiciones generales de los procesos de hábeas corpus, amparo, hábeas data y cumplimiento; y posteriormente, en su título cuarto algunas disposiciones específicas del proceso de hábeas data.

Específicamente este título establece que este proceso pretende[167] proteger los derechos de acceso a la información y de *"conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados (…) Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales"* (Congreso de la República del Perú, 2004).

El Código Procesal Constitucional peruano establece además como requisito especial de la demanda que el interesado haya reclamado el respeto de sus derechos por parte del procesador de datos, mas no exige que el demandante agote la vía administrativa para imponer la acción de habeas data. Asimismo, el Código permite que el Juez en el

[167] El Tribunal Constitucional ha manifestado que el habeas data en Perú procura fundamentalmente reparar el daño causado al individuo (Tribunal Constitucional de la República del Perú, 1996).

proceso pueda requerir que el demandado aporte información de cualquier tipo que resulte conducente a la resolución de la causa. Finalmente, establece que el procedimiento por seguir será el mismo que el seguido en un proceso de amparo, siendo este adaptable a las circunstancias del caso.

Según la jurisprudencia constitucional peruana en este país es posible identificar actualmente los siguientes tipos de habeas data:

1. "***Hábeas Data Puro:*** *Reparar agresiones contra la manipulación de datos personalísimos almacenados en bancos de información computarizados o no.*

   ***1.1. Hábeas Data de Cognición:*** *No se trata de un proceso en virtud del cual se pretende la manipulación de los datos, sino efectuar una tarea de conocimiento y de supervisión sobre la forma en que la información personal almacenada está siendo utilizada.*

   ***1.1.1. Hábeas Data Informativo:*** *Está dirigido a conocer el contenido de la información que se almacena en el banco de datos (qué se guarda).*

   ***1.1.2. Hábeas Data Inquisitivo:*** *Para que se diga el nombre de la persona que proporcionó el dato (quién).*

   ***1.1.3. Hábeas Data Teleológico:*** *Busca esclarecer los motivos que han llevado al sujeto activo a la creación del dato personal (para qué).*

   ***1.1.4. Hábeas Data de Ubicación:*** *Tiene como objeto que el sujeto activo del poder informático responda dónde está ubicado el dato, a fin de que el sujeto pasivo -el accionante- pueda ejercer su derecho (dónde).*

   ***1.2. Hábeas Data Manipulador:*** *No tiene como propósito el conocimiento de la información almacenada, sino su modificación.*

   ***1.2.1. Hábeas Data Aditivo:*** *Agrega al banco de datos una información no contenida. Esta información puede consistir: en la actualización de una información*

*cierta pero que por el paso del tiempo se ha visto modificada; también puede tratarse de una información que tiene como objeto aclarar la certeza de un dato que ha sido mal interpretado; o incorporar al banco de datos una información omitida que perjudica al sujeto pasivo.*

***1.2.2. Hábeas Data Correctivo:*** *Tiene como objeto modificar los datos imprecisos y cambiar o borrar los falsos.*

***1.2.3. Hábeas Data Supresorio:*** *Busca eliminar la información sensible o datos que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona. También puede proceder cuando la información que se almacena no guarda relación con la finalidad para la cual ha sido creado el banco de datos.*

***1.2.4. Hábeas Data Confidencial:*** *Impedir que las personas no autorizadas accedan a una información que ha sido calificada como reservada. En este tipo, se incluye la prohibición de datos que por el paso del tiempo o por sentencia firme se impide su comunicación a terceros.*

***1.2.5. Hábeas Data Desvinculador****: Sirve para impedir que terceros conozcan la identificación de una o más personas cuyos datos han sido almacenados en función de determinados aspectos generales como la edad, raza, sexo, ubicación social, grado de instrucción, idioma, profesión.*

***1.2.6. Hábeas Data Cifrador:*** *Tiene como objeto que el dato sea guardado bajo un código que sólo puede ser descifrado por quien está autorizado a hacerlo.*

***1.2.7. Hábeas Data Cautelar:*** *Tiene como propósito impedir la manipulación opublicación del dato en el marco de un proceso, a fin de asegurar la eficacia del derecho a protegerse.*

***1.2.8. Hábeas Data Garantista:*** *Buscan el control técnico en el manejo de los datos, a fin de determinar si el sistema informativo, computarizado o no, garantiza la*

*confidencialidad y las condiciones mínimas de seguridad de los datos y su utilización de acuerdo con la finalidad para la cual han sido almacenados.*

***1.2.9. Hábeas Data Interpretativo:*** *Tiene como objeto impugnar las valoraciones o conclusiones a las que llega el que analiza la información personal almacenada.*

***1.2.10. Hábeas Data Indemnizatorio:*** *Aunque no es de recibo en nuestro ordenamiento, este tipo de habeas data consiste en solicitar la indemnización por el daño causado con la propalación de la información.*

***2. Habeas Data Impuro:*** *Solicitar el auxilio jurisdiccional para recabar una información pública que le es negada al agraviado.*

***2.1. Hábeas Data de Acceso a Información Pública:*** *Consiste en hacer valer el derecho de toda persona a acceder a la información que obra en la administración pública, salvo las que están expresamente prohibidas por la ley" (Tribunal Constitucional Peruano, 2007).*

En cuanto a su marco legal, Perú cuenta con varias leyes relacionadas con el habeas data, específicamente la Ley Orgánica del Tribunal Constitucional; la Ley 26470 (que realiza una reforma constitucional sobre la Acción de Hábeas Data); la Ley 27806 sobre Transparencia y Acceso a la Información Pública (específicamente las disposiciones generales establecidas del artículo 1 al artículo 11); y la Ley 27444 del Proceso Administrativo General, que del artículo 131 a 134 establece los plazos y términos a los cuales se refiere el Código Procesal Constitucional.

Finalmente se deberá mencionar la recientemente aprobada Ley 29733 de Protección de Datos Personales (Congreso de la República del Perú, 2011) y su reglamento (Presidente de la República del Perú, 2013). Dicha ley consta de un título preliminar

con disposiciones generales y 7 títulos en los que más de 40 artículos procuran regular la materia. Esta ley establece varios de los principios ya vistos en otras legislaciones, tales como la necesidad de información suficiente y consentimiento previo, informado, expreso e inequívoco (y escrito en caso de datos sensibles). Asimismo resulta fundamental señalar que según esta ley las telecomunicaciones, sistemas informáticos o sus diversos instrumentos de carácter privado solamente podrán ser incautados, abiertos, interceptados o intervenidos mediante orden judicial que cumpla con las garantías constitucionales correspondientes.

Asimismo, tanto la ley como su reglamento establecen claras disposiciones en materia de flujos transfronterizos de datos personales, seguridad del tratamiento de datos personales, confidencialidad, derechos del titular de los datos, bancos de datos personales (creación, modificación, cancelación y prestación de los servicios), la creación de la Autoridad Nacional de Protección de Datos Personales y las infracciones correspondientes en caso de violaciones a los datos personales de los administrados.

### Argentina

Se debe caracterizar el caso de Argentina como particular (y ejemplar) en tanto cuenta con un sistema de habeas data de gran calidad, al punto que a la fecha es miembro del

reducido grupo de países americanos[168] cuyo sistema de protección de datos ha sido formalmente reconocido[169] como adecuado, por la Comisión Europea.

La República Argentina cuenta, al igual que los países anteriormente estudiados, con un sistema legal basado en el reconocimiento constitucional del habeas data. En el caso argentino, la Constitución Política establece que este debe ser realizado por medio de la acción de amparo (Flores Dapkevicius, 2005), *"Contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta derechos y garantías (…) Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística*" (Congreso General Constituyente de la Nación Argentina, 1995).

Esta garantía constitucional fue posteriormente regulada por la ley argentina Nº 25326, la cual establece, (junto con el decreto regulatorio Nº 1558/2001 y más de 50 normas que la modifican o complementan[170]) el marco fundamental de la protección de datos personales. Esta ley, titulada Ley de Protección de los Datos Personales, tiene como objeto la "*protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las*

[168] Junto a Uruguay y Canadá.
[169] Ver la Decisión de la Comisión Europea en (Comisión Europea, 2003).
[170] Las cuales pueden verse mencionadas en el Anexo I del documento titulado "Marco Regulatorio de la Protección de Datos en Argentina" (The 3M Company, 2011).

*personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional*" (Congreso de la Nación Argentina, 2000) y es aplicable tanto a los datos de personas físicas como jurídicas.

La ley Nº 25326 reconoce, entre otros, los principios de licitud, calidad de los datos, consentimiento, información, pertinencia, exactitud, adecuación, utilización abusiva, categorización de los datos y seguridad de los datos. Asimismo establece limitaciones a las cesiones de los datos con base en los fines perseguidos y, en caso de las transferencias internacionales de datos personales, prohíbe la salida de datos hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados.

Con base en las disposiciones de esta norma, actualmente en Argentina resulta fundamental la inscripción de las bases de datos ante la Dirección Nacional de Protección de los Datos Personales. Y si bien es cierto que la ley no requiere el nombramiento de un oficial corporativo de protección de datos, algunos[171] de los entes que manejen datos personales deberán asignar un *responsable de seguridad* quien se encargará solamente de vigilar las medidas de seguridad de la información aplicables a las bases de datos.

En materia de consentimiento, la legislación Argentina establece que el consentimiento debe ser escrito, libre e informado, más no será necesario cuando sea recopilado de fuentes públicas con acceso irrestricto; recopilado por el gobierno;

[171] Todos aquellos entes que manejen datos con requisitos de seguridad medios o altos deben nombrar un Responsable de Seguridad. (Campbell, Giay, & Peruzzotti, 2012).

derive de una relación directa con el sujeto (y sea necesario para tal relación); sea necesario para transacciones financieras o incluya tan solo el nombre, número de identidad, números de seguro social o de identificación fiscal, ocupación, fecha de nacimiento y domicilio.

En materia de seguridad de la información, la ley establece la obligación del responsable o usuario del archivo de datos de *"…garantizar la seguridad y confidencialidad de los datos personales para evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información…"* (Congreso de la Nación Argentina, 2000). Además, deben cumplirse las disposiciones que en materia de seguridad de la información establece la Disposición No. 11/2006 dictada por el Poder Ejecutivo, la cual señala medidas como la implementación de tres niveles de seguridad (básico, medio y crítico) por ser determinados conforme la naturaleza de la información (Dirección Nacional de Protección de los Datos Personales, 2006).

Extrañamente, la legislación Argentina vigente no contempla a la fecha el requisito de informar a los sujetos de datos en caso de que existan violaciones a sus datos personales; sin embargo sí establece la obligación de que las compañías registren tales incidentes y los presenten a la Dirección en caso de que esta así lo solicite. A pesar de lo anterior, según Campbell, Giay y Peruzzotti, con base en el principio general de buena fe establecido en el artículo 1198 del Código Civil argentino, el controlador de los datos debería informar al interesado con miras a evitar mayores daños (Campbell, Giay, & Peruzzotti, 2012).

Finalmente, la ley regula tanto las asignaciones y responsabilidades de la Dirección de Protección de los Datos Personales como la acción de protección de los datos personales o hábeas data, la cual procederá *"a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización"* (Congreso de la Nación Argentina, 2000).

Se debe resaltar también que la ley soluciona el problema de la competencia de una manera bastante particular, en tanto establece que será competente para decidir sobre la acción de habeas data *"el juez del domicilio del actor, del domicilio del demandado, el del lugar en que el hecho o acto se exteriorice o pudiera tener efecto a elección del actor"* (Congreso de la Nación Argentina, 2000) y que adquiere competencia federal cuando sea interpuesta contra *"archivos de datos públicos de organismos nacionales y cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales"* (Congreso de la Nación Argentina, 2000).

### Colombia

En el caso de Colombia existe una situación particular en tanto la Constitución Política colombiana de 1991 no hace mención explícita del habeas data sino que se enfoca, a lo largo de sus artículos 15 y 86, en establecer los derechos fundamentales relacionados

con el tratamiento de datos personales y el deber del Estado de ampararlos (Ramírez Salinas, 2003, pág. 19). A pesar de ello, debe considerarse indudable la existencia de un sistema de hábeas data en Colombia, en tanto la jurisprudencia constitucional se encargó posteriormente de recopilar mediante este nombre tales derechos.

El autor Víctor Bazán se ha referido con anterioridad al caso colombiano; en su opinión: *"El hábeas data queda incluido en el capítulo I ("De los derechos fundamentales") del Título II ("De los derechos, las garantías y los deberes") de la Constitución y, al parecer, se lo diseñó en principio para ser canalizado a través de la acción de tutela (equivalente a lo que conocemos por proceso de amparo). Sin embargo, según Cifuentes Muñoz, en rigor el hábeas data corresponde a un específico proceso constitucional, y añade el citado autor que si bien la Corte Constitucional se ha limitado a conferir a la ubicación de los derechos bajo los mencionados capítulo y epígrafe un valor meramente ilustrativo o indicativo de la naturaleza de determinado derecho –no enteramente conclusivo-, no se ha puesto jamás en duda que el hábeas data ostente la condición de derecho fundamental"* (Bazán, 2012, pág. 45)[172].

A pesar de esta situación, desde 1991 hasta mediados de la década del 2000 (Privacy International, 2006), Colombia no contaba con una ley general sobre el tema, que estableciera principios básicos sobre protección de datos por ser aplicados en un nivel general en el sistema legal; si bien es cierto que podían ser encontrados algunos ejemplos de normas sectoriales relevantes, ello no era suficiente como para aseverar que existiera en dicho país un nivel adecuado de protección a los datos personales (Remolina-Angarita, 2010, pág. 502).

[172] Sobre el tema, véase la sentencia C-748 de 2011 de la Corte Constitucional de Colombia.

Frente a tal situación, a partir del año 2008 el Congreso de la República de Colombia comenzó a promulgar leyes dirigidas a desarrollar el habeas data y la protección de datos personales, como lo son la Ley 1266 de 2008 (Congreso de la República de Colombia, 2008), la Ley 1273 de 2009 (Congreso de la República de Colombia, 2009), la Ley 1581 de 2012 (Congreso de la República de Colombia, 2012) y la ley 1621 de 2013 (Congreso de la República de Colombia, 2013).

La primera de estas leyes se encontraba dirigida fundamentalmente a crear disposiciones generales del Derecho Constitucional de todas las personas al hábeas data y el manejo de la información contenida en bases de datos personales; en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Para ello la ley establece principios de la administración de datos[173], los derechos de los titulares de la información, los deberes de los operadores, las fuentes y los usuarios de información, disposiciones específicas relativas a los bancos de datos de información[174], normas en materia de peticiones de consultas y reclamos y las bases sobre la vigilancia de los destinatarios de la ley[175] (Congreso de la República de Colombia, 2008).

La Ley 1273 de 2009 se caracteriza por crear un nuevo bien jurídico tutelado, denominado “de la protección de la información y de los datos”, mediante el cual se procura preservar la confidencialidad, la integridad, la seguridad y la disponibilidad de

[173] Como veracidad o calidad de los registros o datos, finalidad, circulación restringida, temporalidad de la información, interpretación integral de derechos constitucionales, seguridad y confidencialidad.
[174] Tales como el establecimiento del llamado “Principio de favorecimiento a una actividad de interés público”, la creación de ciertos requisitos especiales para los operadores y fuentes, el contenido de la información, y el acceso a la información por parte de los usuarios.
[175] Para ser ejercida por la Superintendencia Financiera de Colombia y la Superintendencia de Industria y Comercio.

los datos y de los sistemas informáticos del país, incluyéndose dentro de estos los datos personales. Legislación ejemplar por sus avances en la regulación del Derecho Informático, la ley 1273 incluye disposiciones que castigan el acceso abusivo a sistemas informáticos; la obstaculización ilegítima de los sistemas informáticos y de las redes de telecomunicaciones; la interceptación de datos informáticos; la suplantación de sitios web para capturar datos personales y la transferencia no consentida de activos; entre otros.

Por su parte, la Ley Estatutaria 1581 de 2012 se dirigió a formular disposiciones que afectarían la protección de datos personales de manera más general, complementando la protección brindada por la ley 1266[176] y fortaleciendo de esta manera el marco legal colombiano sobre el tema. Dentro de las disposiciones fundamentales de esta ley se encuentra el reforzamiento del papel de la Superintendencia de la Industria y Comercio; la creación de un registro público nacional de bases de datos; la diferenciación entre datos personales y datos personales sensibles; el requerimiento de consentimiento informado previo a la recolección y procesamiento de datos; la prohibición de procesar datos sensibles (salvo con consentimiento del interesado); la prohibición general de datos a países que no cuenten con medidas adecuadas de protección (con algunas excepciones); el establecimiento de disposiciones en materia de seguridad de la información, y la obligación del procesador de informar al interesado en caso de que se den violaciones a sus datos personales (BakerHostetler, 2013, págs. 41-43).

[176] Si bien las disposiciones de la ley 1581 establecen explícitamente que esta no regula las bases de datos comprendidas por la ley 1266.

Finalmente, la ley 1621 de 2013 fue creada con miras a fortalecer el marco jurídico que permite a los organismos de inteligencia y contrainteligencia cumplir con su misión constitucional, para lo cual establece disposiciones que, entre otros temas se relacionan con el monitoreo del espectro electromagnético y la interceptación de comunicaciones privadas[177], a la vez que establece centros de protección de datos de inteligencia y contrainteligencia en el país.

Se puede concluir señalando que en términos generales el sistema de protección de datos implementado actualmente en Colombia es robusto, y si bien cuenta con defectos y omisiones que impiden su certificación de adecuación a los estándares europeos en la materia, plantea una buena cantidad de disposiciones novedosas que deberán ser consideradas en cualquier proyecto de reforma legislativa que plantee nuestro país.

### *Adopción Nacional de Normativa Especializada*

En cuarto lugar en este estudio del Derecho comparado se encuentran aquellos países que cuentan con legislación específica dirigida a regular la aplicación de las técnicas y herramientas iusinformáticas de protección de datos personales.

Popularizado especialmente en los últimos años, el movimiento de regulación legal de la protección de datos personales surge en América principalmente como respuesta a

[177] Para lo que obliga a los operadores de servicios de telecomunicaciones a brindar su completa colaboración a las instituciones relevantes, facilitando dentro de otros elementos los datos técnicos de identificación y localización de los subscriptores investigados.

los vacíos existentes en los sistemas que utilizan únicamente el habeas data, y en el resto del mundo como una solución a las necesidades evidenciadas por los fenómenos globales asociados con las tecnologías de la información y la comunicación.

Teniendo en consideración este contexto, es posible asegurar que en este último apartado se podrá encontrar la mayor parte de los países del mundo que procuran generar por sus propios medios (o emulando a otros países) herramientas dirigidas a la protección de los datos personales. Debido a esta situación se puede encuadrar dentro de este grupo a una gran cantidad de países que actualmente brindan los más diversos niveles de protección a los interesados.

Este apartado se encuentra fundamentalmente dirigido a evidenciar la necesidad de estandarización y armonización existente en las legislaciones internacionales sobre protección de datos personales. Por ello, a continuación se examinarán los ejemplos de cinco países que cuentan en la actualidad con leyes sobre el tema; a saber: España[178], Canadá, México, Japón y China.

## España

Enmarcado dentro del ámbito de aplicación de las diversas directivas europeas ya aplicadas, el marco normativo vigente en España en materia de protección de datos

[178] Debe reconocerse que el ejemplo español se encuentra enmarcado dentro del Sistema Europeo de Protección de Datos Personales, por lo que su estudio a lo largo de la presente sección podría parecer extraño. A pesar de lo anterior, procederemos a estudiar la legislación de este país por dos motivos fundamentales: 1) su cercanía con la legislación costarricense sobre la materia; y 2) la necesidad de ejemplificar los dos extremos de protección posibles mediante la adopción nacional de leyes relacionadas con el tema.

personales se encuentra basado, en primer lugar, en el reconocimiento constitucional de la intimidad personal, el secreto de las comunicaciones y la protección de los datos personales que tutela el artículo 18 de su Constitución Política.

En segundo lugar, resulta necesario mencionar dentro de este estudio del sistema español la llamada "Ley Orgánica de Protección de Datos de Carácter Personal" (LOPD), ley dirigida a armonizar el sistema español con las disposiciones de la Directiva Europea de Protección de Datos Personales y que fundamentalmente procura *"garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar"* (Congreso de los Diputados, 1999, pág. 1).

Básica dentro del actual sistema de protección de datos español, la LOPD se fundamenta en los principios de adecuación, pertinencia, no excesividad, finalidad, exactitud, actualidad, oficiosidad, finalidad, seguridad y legalidad; y con base en los anteriores establece los derechos aplicables para el sujeto de datos, como por ejemplo: el tener conocimiento cuando sus datos sean utilizados por el sector público o privado y acceder, corregir o solicitar la destrucción de los datos incorrectos dentro de estas bases de datos (Privacy International, 2011).

Establece también disposiciones relativas a los datos sensibles de los interesados, con respecto a los cuales establece una serie de restricciones a su tratamiento así como excepciones a dichas restricciones (específicamente en materia de salud). Por otro lado, también contempla la LOPD disposiciones en materia de seguridad de los datos, deber de secreto, acceso a los datos por cuenta de terceros, impugnación de

valoraciones[179], derecho a indemnización y algunas reglas específicas aplicables tanto a ficheros de titularidad pública como privada.

En materia del movimiento internacional de datos, mantiene la norma española como regla general que *"no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley" (Congreso de los Diputados, 1999, pág. 21),* y establece como ente encargado de decidir sobre dicho nivel de protección a la Agencia de Protección de Datos, creada por esta misma ley en su artículo 35[180].

La LOPD ha sido complementada a lo largo de los años por algunos *decretos reales* dirigidos a fortalecer su aplicación; dentro de ellos se deben mencionar fundamentalmente el Decreto Real del 19 de enero de 2008 (Agencia Española de Protección de Datos, 2008), dirigido a prevenir el uso de datos personales sin consentimiento del sujeto de datos y a incrementar las medidas de seguridad aplicables a diversos tipos de datos personales; el Decreto Real 1720/2007 (Agencia Española de Protección de Datos, 2008) que implementa y aumenta las disposiciones de la LOPD, específicamente en materia de consentimiento de menores de edad, medidas de seguridad en bases de datos manuales, procedimientos administrativos relacionados y transferencias internacionales de datos personales; y el Decreto Real

[179] Derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

[180] A la cual asigna también las funciones de: emitir autorizaciones para el procesamiento, vigilar el cumplimiento de la Ley, manejar las quejas de los individuos, educar al público, establecer penas ante violaciones a la ley, publicar la existencia de datos personales, reportar al ministerio de justicia, monitorear y adoptar autorizaciones para transferencias internacionales de datos (y cooperar con las agencias internacionales relevantes al tema), y vigilar el cumplimiento de las disposiciones en materia de datos estadísticos (Leiva, 2012).

3/2010 (Agencia Española de Protección de Datos, 2010) dirigido a evitar el intercambio de datos sin consentimiento del interesado.

### Canadá

Loable por ser uno de los pocos países del continente americano que cuenta con la certificación de protección adecuada mediante los estándares europeos, Canadá puede ser caracterizado como un país que cuenta con un robusto sistema de protección de datos, cuya efectividad no se ha visto amedrentada por no contar con disposiciones constitucionales que lo sustenten[181].

Las principales disposiciones que en el nivel Federal rigen la protección de datos en Canadá son la Privacy Act (Ministerio de Justicia de Canadá, 2014) y la Personal Information Protection and Electronic Documents Act (PIPEDA) (Ministerio de Justicia de Canadá, 2014). Estas leyes se encuentran acompañadas actualmente por la Library and Archives of Canada Act (Ministerio de Justicia de Canadá, 2014), la cual se relaciona con la retención y eliminación de la información personal por las instituciones gubernamentales (Organización de Estados Americanos, 2012, pág. 20); y por un Código Modelo para la Protección de la Información Personal (Canadian Standards Association, 1996) que actualmente constituye el principal referente en

[181] La sección 8 de la Declaración de Derechos y Libertades (la cual forma parte de la constitución Canadiense) contempla el elemento constitucional más cercano a la Protección de Datos Personales al establecer el derecho a la seguridad contra registros e incautaciones irrazonables. A partir de un examen contextual amplio, las cortes canadienses han logrado desarrollar a partir de este derecho todo un sistema de protección a las expectativas razonables de intimidad individual (Organización de Estados Americanos, 2012).

materia de autorregulación en el país y no solamente ha sido incorporado dentro de PIPEDA, sino que también en la actualidad es un estándar nacional en Canadá.

- Privacy Act: vigente desde 1983, la Privacy Act define las obligaciones del gobierno federal en materia de recolección, uso, publicación, retención y eliminación de la información personal. Con tal fin esta ley establece un número de disposiciones dentro de las cuales otorga a los individuos el derecho de acceso y rectificación de su información personal, establece un *comisionado de privacidad* y asegura los casos en los que el afectado puede recurrir ante las cortes para defender sus derechos (Organización de Estados Americanos, 2012, pág. 20).
- Personal Information Protection and Electronic Documents Act (PIPEDA): la cual se relaciona con la recolección, uso y liberación de información personal por parte del sector privado en sus actividades comerciales, siendo esta aplicable a todos los sectores regulados por la jurisdicción federal (incluyendo telecomunicaciones). Dentro de sus principales disposiciones, la ley brinda el control sobre la información personal a los interesados, a quienes les reconoce el derecho de otorgar o no su consentimiento informado; así como los derechos de acceso y rectificación. Por otro lado, define al *comisionado de privacidad* como encargado de la investigación de anomalías y la resolución de controversias; de estas últimas, las no resueltas quedan por medios alternos ante la jurisdicción de las cortes federales (Organización de Estados Americanos, 2012, pág. 20).
- Código Modelo para la Protección de la Información Personal: el cual se basa en diez principios fundamentales para asegurar la protección de la información personal, a saber: responsabilidad; identificación de propósitos; consentimiento;

limitación de la recolección; limitación del uso, liberación y retención; fidelidad; salvaguardas; apertura; acceso individual y desafío del cumplimiento[182] (Canadian Standards Association, 1996).

Finalmente, se debe recordar que las disposiciones de PIPEDA han sido consideradas como adecuadas mediante los estándares europeos desde el 20 de septiembre de 2001 (Comisión Europea, 2001); estas consideraciones fueron confirmadas en 2006 y en 2005 fueron también consideradas como adecuadas las disposiciones del Gobierno de Canadá en materia de manejo de listas de pasajeros por vías aéreas (Organización de Estados Americanos, 2012, pág. 27).

### México

El marco legal mexicano gira, en materia de protección de datos, alrededor del artículo 16 de la Constitución Política de 1917, el cual fue objeto de una reforma realizada en 2009 con miras a extender a todo ciudadano los derechos necesarios para acceder, corregir, cancelar u oponerse al mal manejo o publicación ilícita de sus datos personales. Asimismo, según las disposiciones del Artículo 73 XXIX-O constitucional, corresponde al Congreso Federal el *"legislar en materia de protección de datos personales en posesión de particulares" (Congreso Constituyente de México, 1917).*[183]

[182] Relativo a la capacidad del individuo de elevar sus dudas sobre el cumplimiento de la organización ante el encargado de protección de datos de la organización en cuestión (Canadian Standards Association, 1996, pág. 20).

[183] Dichas disposiciones son complementadas por otros derechos consagrados constitucionalmente como lo son el secreto de las comunicaciones, la supeditación a órdenes judiciales de las escuchas telefónicas y demás límites a la injerencia administrativa en los ámbitos íntimos del hogar.

El marco constitucional conformado por los artículos supracitados constituye el fundamento para las diversas leyes federales que rigen la materia en México. Específicamente, dirige (en los aspectos relacionados con la protección de datos personales) la aplicación de leyes como la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Cámara de Diputados del H. Congreso de la Unión, 2002), la Ley Federal de las Entidades Paraestatales (Cámara de Diputados del H. Congreso de la Unión, 1986), la Ley Federal de Procedimiento Administrativo (Cámara de Diputados del H. Congreso de la Unión, 1994), la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos (Cámara de Diputados del H. Congreso de la Unión, 2002) y especialmente las disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Cámara de Diputados del H. Congreso de la Unión, 2010).

En la actualidad es posible afirmar que México cuenta con un cuerpo normativo sólido en materia de protección de datos personales, dentro del cual se destacan por su relevancia con el presente tema de investigación, las ya mencionadas: Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y la Ley Federal de Protección de Datos en Posesión de los Particulares, las cuales serán analizadas con mayor profundidad a continuación.

Publicada por primera vez en el Diario Oficial de la Federación el 11 de junio de 2002 y reformada por última vez en junio del 2012, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental *"regula el derecho de todos a accesar a información mantenida por cuerpos gubernamentales y establece los criterios, procedimientos y principios*

*por medio de los cuales el derecho de acceso puede ser ejercido frente a autoridades federales"* (Privacy International, 2013, pág. 5). Para ello comienza por establecer obligaciones de máxima transparencia para los entes federales, delimita lo que comprenderá como información reservada y confidencial, a la vez que establece disposiciones relativas a la protección de datos personales por ser aplicadas ante cualquier solicitud de liberación de información pública gubernamental (artículos 20 a 26).

A lo largo de dichos artículos, la ley establece la obligación de adoptar procedimientos adecuados; tratar datos personales solo cuando estos sean adecuados; poner a disposición de los interesados los propósitos del tratamiento; procurar que los datos sean exactos y actualizados; sustituir, rectificar o completar los datos inexactos; adoptar medidas de seguridad de la información; no difundir, distribuir o comercializar los datos personales salvo mediante consentimiento expreso; informar al Instituto Federal de Acceso a la Información y Protección de Datos (creado por el Artículo 33 de esta ley) cuando posean sistemas de datos personales y proporcionar a los interesados o sus representantes las informaciones o datos que obren en un sistema de datos personales bajo su tutela.

Por su parte, la Ley Federal de Protección de Datos, publicada el 5 de julio de 2010 constituye el pilar fundamental del sistema de protección de datos personales mexicano, mediante el cual se unifican, por primera vez en un nivel federal, *"obligaciones para compañías y entidades privadas que recolectan, procesan, almacenan o manejan datos personales, delineando reglas, requisitos y disposiciones tendientes a asegurar el tratamiento correcto de los datos personales" (Privacy International, 2013, pág. 5).*

Caracterizada por tener un ámbito de aplicación limitado al territorio nacional mexicano (independientemente del lugar de residencia de los sujetos de datos) y por no discriminar en razón de la nacionalidad de los sujetos de datos, la Ley Federal de Protección de Datos supera diversas de las limitaciones del sistema de habeas data al comprender dentro de sus disposiciones al individuo como el dueño de sus datos y como poseedor de todos los derechos relevantes al uso de tales datos. Más aún, debe ser recalcada la presente ley por incorporar disposiciones expresas tendientes al reconocimiento de los estándares internacionales vigentes en materia de protección de datos, reconociendo el hecho de que México es firmante de las Directrices de las Naciones Unidas para la Regulación de Archivos de Datos Personales.

Finalmente, se debe reconocer que el marco normativo mexicano alcanza en muchos sentidos los niveles exigidos por la Unión Europea[184] y por otros países tan exigentes en la materia como Canadá. Asimismo, se debe recordar que el sistema Mexicano cuenta también con una gran cantidad de elementos regulatorios sobre la materia, que no solamente se limitan al nivel federal, sino que han sido creados e implementados por los diversos estados miembros de la Unión. Por tal situación[185] no es extraño encontrar en las diversas páginas de compañías basadas en su territorio declaraciones de privacidad que superan los mínimos establecidos por su legislación federal, y se encuentran en ellos usualmente disposiciones relativas a *cookies* y a las aplicaciones móviles aún cuando la ley no se refiera expresamente a dichos puntos.

[184] A pesar de ello, este país no cuenta aún con la certificación oficial de protección adecuada bajo los estándares europeos.
[185] Aunada también con la cercanía comercial de este país con la Unión Europea.

## Japón

El sistema japonés de protección de datos se caracteriza por contar con fundamentos puramente legales, dentro de los cuales se incluye la filosofía y políticas básicas, así como las *"funciones y medidas a ser tomadas tanto por el gobierno del estado como por los gobiernos locales" (Komukai, 2013, pág. 3),* las cuales serán posteriormente adoptadas tanto por el sector público como por el sector privado. En términos generales se puede afirmar que en Japón la norma fundamental en la materia es la Ley sobre Protección de Información Personal Número 57 de 2003 (個人情報の保護に関する法律 ) *(Ministerio de Justicia de Japón, 2009),* la cual ha sido complementada por más de dos mil directrices emitidas por gobiernos locales y municipalidades.

Aplicable a toda información sobre un individuo con vida que pueda servir para identificarle, la Ley se fundamenta en el hecho de que la información personal debe ser manejada cautelosamente bajo la filosofía de respeto al individuo, por lo que promueve el manejo adecuado de la información personal (artículo 3) mediante el establecimiento de guías generales que servirán posteriormente como fundamento para la creación de reglas específicas por parte de los ministerios[186].

[186] N. del A. en este caso debemos aclarar que el funcionamiento de la norma en cuestión se diferencia bastante del sistema empleado en nuestro país y se acerca más al sistema de directivas empleado en la Unión Europea. Esto debido a que la ley establece un conjunto de directrices fundamentales que serán posteriormente aplicadas dentro de la regulación administrativa vinculante que es creada por cada uno de los ministerios de gobierno. Dicha regulación administrativa deberá ser posteriormente aplicada por los sectores privados que se encuentren supeditados a cada ministerio, así encontraremos que en realidad los entes gubernamentales encargados de la formación normativa en materia de protección de datos en Japón son ministerios como los de Economía, Comercio e industria; Salud, Trabajo y Bienestar; Asuntos Interiores y Comunicaciones; Tierras, Infraestructura y Transporte y la Agencia de Servicios Financieros (BakerHostetler, 2013, pág. 105).

Comenzando por el establecimiento de las responsabilidades de Estado y de los gobiernos locales, y la regulación de las políticas básicas sobre la materia[187], la Ley establece la necesidad de brindar apoyo a los gobiernos locales (especialmente en el procesamiento de quejas relacionadas con el tema) así como la obligación de dichos gobiernos de mediar entre los operadores de información personal y los interesados.

Asimismo, la Ley establece las obligaciones para las entidades que manejen información personal, dentro de las cuales se incluyen las siguientes (Ministerio de Justicia de Japón, 2009):

- La obligación de especificar el propósito de la utilización.
- La restricción del uso supeditada a dicho propósito.
- La prohibición de formas ilegítimas de recopilación de información personal.
- Notificar al interesado sobre la recopilación de sus datos.
- El mantenimiento y actualización de los datos para asegurar su precisión.
- El ajustarse a las diversas medidas de seguridad de la información aplicables.
- Supervisar a los empleados y socios en el tratamiento de los datos personales.
- Acatar las restricciones sobre transmisión de los datos a terceros.
- Brindar información a los interesados sobre el operador que maneja sus datos, el propósito de dicho tratamiento y los procedimientos relevantes a disposición del interesado.

[187] Que comprenderá la dirección básica de promoción de medidas para la protección de información personal, las medidas de protección a ser tomadas por el Estado, gobiernos locales, agencias administrativas, entidades que manejen información personal, el manejo de quejas y otros asuntos importantes relativos a las medidas de protección de información personal.

- El acatar las disposiciones sobre acceso a la información (artículo 25), corrección de los datos (artículo 26) y eliminación (artículo 27).
- El procesar de manera adecuada y expedita las quejas que se le presenten.
- Seguir las recomendaciones y órdenes del ministerio competente[188].

Por otra parte, a Ley también contempla disposiciones relevantes a las comunicaciones electrónicas, como por ejemplo: el requerir que en caso de que se utilicen *cookies* o sistemas similares para recolectar información, el propósito de tal recolección sea notificado al interesado. Además, debe señalarse que si bien la Ley no hace mención explícita a la transferencia internacional de datos personales, sus disposiciones en materia de cesión de datos personales a terceros seguirán siendo aplicables; por lo que se considera necesario el consentimiento del interesado para que estas puedan ser llevadas a cabo (Carter & Miyata, 2012).

Finalmente, debe resaltarse que la Ley posee algunos elementos característicos como el asignar el papel de *ente regulador* a los diversos ministerios relevantes y el no contar con una norma general sobre deber de notificar en caso de violaciones a los datos personales. Ante esta realidad Japón se encuentra actualmente discutiendo la necesidad de reformar o renovar su normativa en materia de protección de datos personales (Komukai, 2013, págs. 6-11).

[188] La ley contempla un número de remedios a las violaciones de los datos personales, dentro de los cuales podemos encontrar el establecimiento de multas y la imposición de penas de prisión (con trabajo forzado) hasta por seis meses a quienes no cumplan con las órdenes dirigidas a corregir las violaciones. Con respecto a los interesados, la ley les asigna también los derechos a establecer quejas y a exigir el pago de daños por vía judicial en caso de que estos les fueran sean aplicables.

## China

El marco legal que sustenta la protección de datos personales en China es relativamente limitado; esto en tanto a la fecha no es posible identificar una ley general que regule el tema en su totalidad. Si bien es cierto que en la Constitución Política de la República del Pueblo de China es posible encontrar disposiciones relativas a la dignidad (artículo 38), la protección de la libertad (artículo 37), lugar de residencia (artículo 39) y a la libertad y privacidad de la correspondencia de sus ciudadanos (artículo 40), no es posible identificar una norma constitucional que manifieste el derecho a la intimidad o la privacidad en este país.

Esta situación no ha pasado inadvertida por un pueblo como el chino que se caracteriza por estar cara vez más consciente de los problemas que le aquejan, en especial dada su creciente integración con el resto del mundo. Es por ello que, según Privacy International, el gobierno Chino ha prometido ya en diversas ocasiones que habrá de actualizar su marco regulatorio, con miras a incorporar de mejor manera los derechos humanos dentro de su Constitución Política y en el resto de su marco legal (Privacy International, 2012).

En todo caso, resultaría imposible aseverar que actualmente China no posee herramientas legales dirigidas a la protección a los datos personales. En la actualidad este país cuenta fundamentalmente con una serie de normas estatutarias dirigidas a tratar este problema (aunque sea de manera indirecta), dentro de las cuales se puede encontrar el artículo 101 de los Principios Generales de la Ley Civil (el cual establece el derecho de la reputación de individuos y empresas), la reforma de varios artículos de

su código penal (Winton, Zhang, Innes-Stubb, & Xu, 2012) y las reformas realizadas a la Ley de Responsabilidad Extracontractual (que permiten a los ciudadanos demandar el pago de daños sufridos por violaciones a su privacidad) (Privacy International, 2012).

Como parte de sus esfuerzos por actualizar su sistema normativo, en los últimos años China ha generado también dos elementos legales que constituyen un primer paso hacia la regulación directa de la protección de datos personales. Se trata específicamente a la "Decisión sobre el Fortalecimiento de la Protección de la Información en Internet" (McDermott Will & Emery, 2013) y las "Guías para la protección de la información personal en sistemas de información para servicios públicos y comerciales" (Greenleaf & Tian, 2013).

Único elemento vigente a la fecha con carácter vinculante, la Decisión sobre el Fortalecimiento de la Protección de la Información en Internet, fue adoptada por el Comité Permanente de la Asamblea Popular Nacional con miras a *"proteger la seguridad de la información en Internet, salvaguardar los derechos legítimos e intereses de los ciudadanos, las personas jurídicas y otras organizaciones, y mantener la seguridad nacional y el interés público" (Ishimaru & Associates LLP, 2012).*

La decisión incluye 12 artículos que establecen básicamente que:

- El Estado protegerá la información electrónica capaz de identificar a los individuos (y prohíbe la recopilación y distribución ilegal de dichos datos).
- Los proveedores de Internet y los entes que recopilen o utilicen tales informaciones deben seguir los principios de legalidad, oportunidad y necesidad, a la vez que explican claramente cómo utilizarán dicha información a los interesados.

- Quienes traten con datos personales deben mantener una estricta confidencialidad sobre el contenido de estos.
- Deben ser adoptadas las medidas técnicas y necesarias para proteger la seguridad de la información y prevenir su desmejoramiento o liberación.
- En caso de que el proveedor descubra una fuga de información personal esta deberá cesar inmediatamente y ser reportada a la agencia competente.
- Los proveedores de internet y telecomunicaciones en general, deberán requerir que sus usuarios les faciliten su identidad real en el momento de contratar tales servicios.
- Prohibición a las comunicaciones no deseadas al usuario.
- Establece para todo usuario que encuentre en internet informaciones que afecten sus derechos e intereses legítimos, el derecho de exigir de su proveedor de servicios de internet el cese de la difusión, el borrado o la adopción de aquellas medidas necesarias detener tal afectación.
- Establece el derecho de denunciar conductas criminales relevantes a la información personal y el derecho del afectado de reclamar daños por vía judicial.
- Pena aquellas conductas contrarias a la Decisión con advertencias, multas, confiscaciones, revocación de licencias o registros, eliminación de páginas web, prohibición de ejercer actividades en el negocio de servicios de red y responsabilidad criminal conforme con la ley.

Si bien es cierto que la Decisión constituye el primer esfuerzo normativo realizado por el Estado de la República Popular de China, resulta evidente que su contenido es muy limitado con respecto a las leyes anteriormente estudiadas. La Decisión ha sido

fuertemente criticada en tanto presenta vacíos importantes (no crea un ente regulador, por ejemplo) y contiene elementos que pueden en potencia afectar el derecho de libre expresión (siendo posible para un usuario exigir la eliminación de una página web que infrinja sus intereses, por ejemplo) y la anonimidad del usuario de internet en un país que es conocido por adoptar políticas controversiales en ambos temas (como la adopción de la *gran muralla de fuego* que limita el acceso a ciertas partes del internet a los ciudadanos chinos[189]).

De cualquier manera, se debe admitir que específicamente para el tema de la protección de los datos personales en el contexto chino, la Decisión, supramencionada, es indudablemente beneficiosa. El establecimiento de bases sólidas y de algunos de los principios de la autodeterminación informativa que son logrados mediante la Decisión plantean la posibilidad de armonizar en algún momento futuro el régimen legal vigente en China en la materia con el adoptado por el resto del mundo, y ello ha sido ya reconocido tanto por nacionales como extranjeros (Pappas, 2013).

Finalmente, como ya se mencionara, el gobierno de China (y específicamente el Ministerio de Industria y Tecnologías de la Información) adoptó en noviembre de 2012 una guía no vinculante dirigida a *la protección de la información personal en sistemas de información para servicios públicos y comerciales.* Este documento (solo aplicable a procesamiento automatizado de datos personales) se caracteriza por establecer una división entre datos sensibles y datos personales en general. Adicionalmente establece la necesidad de informar a los interesados afectados por una violación de datos, así como que solamente los datos necesarios podrán ser recopilados para propósitos

[189] Al respecto, ver http://www.greatfirewallofchina.org/ y el FAQ disponible en http://www.greatfirewallofchina.org/faq.php.

específicos y claros, y que estos deberán ser borrados una vez que han cumplido su objetivo (Pisent Masons LLP, 2013).

### *Síntesis de la Segunda Sección*

Modelos Basados en el Habeas Data

*A lo largo de la cual serán examinados los ejemplos de cinco países sudamericanos que protegen los datos personales por medio del habeas data, con miras al establecimiento de un marco contextual que permita comprender su influencia en la región.*

- Las acciones individuales ante una corte constitucional tienen una larga tradición en la historia del Derecho; dentro de los modelos de protección a la autodeterminación informativa existentes en el mundo, el modelo constitucional basado en el habeas data es representativo de los países sudamericanos.
- El concepto de habeas data (tener datos presentes) responde a la acción constitucional que permite al individuo solicitar acceso a bases de datos y ejercer sus derechos de rectificación, actualización, eliminación y olvido.
- Este mecanismo ha sido criticado por su carácter principalmente reparador, que no es ejercido por los interesados sino hasta la etapa de *output* del procesamiento de los datos (en el momento en que se ven afectados por estos).
- Se han estudiado ya a cinco de los países que actualmente siguen el modelo de habeas data en alguna de sus modalidades; a continuación se presentarán sus características fundamentales:
    - Brasil
        - Primer país en introducir el habeas data dentro de su sistema constitucional.
        - Se encuentra fundamentado en los incisos 33 y 72 del artículo 5 de la Constitución Política del país y es complementado por la ley Nº 9.507 del 12/11/1997.
        - En muchos sentidos Brasil cuenta con un sistema aún incompleto de protección de datos personales. A la fecha este país no posee una ley específica sobre protección de datos, ni con un ente regulador especializado en el tema. Tampoco cuenta con disposiciones sobre excepciones a la protección de datos, obligaciones de los controladores de datos, reglas para tipos especiales de datos,

*cookies*, privacidad en dispositivos móviles, procesamiento por terceras partes, transferencias internacionales de datos personales ni contratos modelos regulados legalmente en la materia.

- Este país cuenta actualmente con varios proyectos de ley dirigidos a solventar estos vacíos; quizá el más importante de ellos es el llamado "Marco Civil da Internet", el cual fue recientemente aprobado y desde ya se presenta como una "constitución brasileña del internet" que contempla los ideales de libertad de expresión, neutralidad de la red y protección a la intimidad de los usuarios y de sus datos personales en internet.

- Paraguay
  - País que contempla el habeas data como parte de su artículo 135 constitucional, el cual amplía el texto constitucional brasileño adoptando una mejor definición del habeas data y ampliando la tutela de este instrumento también a áreas de tipo patrimonial.
  - La acción de habeas data en Paraguay implica una garantía constitucional específica que en la práctica debe ser reclamada por medio del amparo genérico y otorga no solamente los derechos al acceso y conocimiento a la información o datos de la persona sino también a la finalidad y uso dados a estos.
  - Procesalmente constituye un proceso más simple que el aplicado en Brasil.
  - A la fecha el país cuenta únicamente con dos leyes relacionadas con el tema (Nº 1682/01 y 1969/02) que establecen disposiciones mínimas especialmente en relación con la información financiera (aunque sí contemplan la protección especial de la información sensible).
  - Aparte de estas disposiciones el marco legislativo paraguayo no cuenta con mayores procedimientos dirigidos a regular la acumulación, retención y liberación de los datos, y con excepción de las pocas disposiciones penales existentes en el código penal del

país, la materia se encuentra aún sin ser regulada debidamente (Privacy International, 2012).

- Perú
  - Contempla disposiciones relativas al tema en los artículos primero y segundo (incisos 5 y 6) de su Constitución Política, la cual establece también el habeas data en el inciso 3 de su artículo 200.
  - Adicionalmente, esta garantía es posteriormente regulada por el título primero del Código Procesal Constitucional peruano, y se ve ampliada por las leyes 26470, 27806, 27444.
  - El caso peruano se presenta como particular pues a pesar de que la jurisprudencia del Tribunal Constitucional ha mencionado en diversas instancias el derecho a la autodeterminación informativa, este derecho ha sido planteado como aquel que brinda al individuo la habilidad de solicitar la rectificación de la información inexacta sobre sí mismo, contenida en bases de datos.
  - Según la jurisprudencia constitucional peruana, en este país son reconocidos los siguientes tipos de habeas data: puro, de cognición, informativo, inquisitivo, teleológico, de ubicación, manipulador, aditivo, correctivo, supresorio, confidencial, desvinculador, cifrador, cautelar, garantista, interpretativo, indemnizatorio, impuro, y de acceso a la información pública.
  - Finalmente, es necesario indicar que en este país fue recientemente aprobada la ley Nº 29773 de Protección de Datos Personales, la cual procura llenar, junto con su reglamento, los vacíos legales existentes en el sistema de habeas data.
- Argentina
  - Miembro del selecto grupo de países americanos cuyo sistema de protección de datos ha sido reconocido como adecuado por la Comisión Europea, este país reconoce constitucionalmente el habeas data, el cual debe ser realizado por medio de la acción de amparo.

- Esta garantía constitucional fue posteriormente regulada por la ley argentina Nº 25326 de Protección de los Datos Personales, la cual establece (junto con el decreto regulatorio Nº 1558/2001 y más de 50 normas que la modifican o complementan) el marco fundamental de la protección de datos personales en este país.
- Esta protección mixta brindada por el sistema argentino ha demostrado su solidez y a la fecha contempla una gran cantidad de disposiciones que desarrollan los múltiples elementos característicamente abarcados por las disposiciones europeas.

o Colombia

- Se caracteriza por el hecho de que su Constitución Política no menciona expresamente el habeas data, sino que se dedica a establecer los derechos fundamentales relacionados con el tratamiento de datos personales y el deber del Estado de ampararlos, los cuales han sido recopilados bajo el título de habeas data por la jurisprudencia constitucional.
- A pesar de esta situación, Colombia no contó con una ley general sobre el tema sino hasta mediados de la década del 2000, cuando el Congreso de la República de Colombia comenzó a promulgar leyes dirigidas a desarrollar el habeas data y la protección de datos personales.
- A la fecha, este país cuenta con cuatro leyes relacionadas específicamente con el tema (Nº 1266, 1273, 1581 y 1621) las cuales tratan los tópicos en relación con la protección constitucional de los datos personales; la incorporación de la protección de la información y de los datos como bienes jurídicos tutelados; el reforzamiento del sistema de protección de datos colombiano, y el fortalecimiento del marco jurídico relativo a las labores de inteligencia y contrainteligencia (fortaleciendo las potestades de retención de datos del país).

Sistemas Basados en Protección Fundamentalmente Legal

*A lo largo de la cual serán examinados los ejemplos de cinco países que han optado por proteger los datos personales por medio de disposiciones de rango legal, con miras a ejemplificar tanto aquellos sistemas que cuentan con niveles aceptables de protección; como aquellos que a la fecha cuentan con legislación muy rudimentaria sobre el tema.*

- España
    - Enmarcado en el ámbito de aplicación de las diversas directivas europeas ya estudiadas, la protección brindada por este país a los datos personales se basa tanto en la interpretación de las disposiciones constitucionales que reconocen el derecho a la intimidad personal, como en la Ley Orgánica de Protección de Datos de Carácter Personal; la cual procura armonizar el sistema español con el sistema europeo y cumplir con los altos estándares exigidos por este.
    - Ha sido complementada a lo largo de los años por algunos decretos reales dirigidos a fortalecer su aplicación, dentro de los cuales se encuentran el Decreto Real del 19 de enero de 2008, el Decreto Real 1720/2007 y el Decreto Real 3/2010.
    - Dentro de sus características fundamentales, la Ley Orgánica procura la aplicación de los principios de adecuación, pertinencia, no excesividad, finalidad, exactitud, actualidad, oficiosidad, finalidad, seguridad y legalidad. Asimismo traslada al ámbito nacional español las disposiciones que en temas como protección de datos sensibles, seguridad de la información, y movimiento internacional de datos requieren las Directivas europeas.
- Canadá
    - Miembro también de los países cuyo sistema de protección de datos ha sido reconocido como adecuado mediante los estándares europeos, el sistema canadiense se fundamenta tanto en la interpretación del derecho constitucional a la seguridad contra registros e incautaciones irrazonables, como en leyes federales y provinciales específicas.

- En el nivel federal, Canadá cuenta con dos leyes de suma importancia: la Privacy Act (la cual define las obligaciones del gobierno federal en materia de recolección, uso, publicación, retención y eliminación de la información personal) y la Personal Information Protection and Electronic Documents Act (que regula el comportamiento del sector privado en la materia).
- Finalmente, Canadá cuenta también con estándares nacionales sobre protección de datos personales que se constituyen en un referente necesario para los esfuerzos de autorregulación, por parte de las compañías domiciliadas en el país.

- México
  - El marco legal mexicano gira, en materia de protección de datos, alrededor de la reforma realizada al artículo 16 constitucional con miras a extender a todo ciudadano los derechos necesarios para acceder, corregir, cancelar u oponerse al mal manejo o publicación ilícita de sus datos personales y a las disposiciones del Artículo 73 XXIX-O constitucional, que asigna al gobierno federal la obligación de legislar en materia de protección de datos personales en posesión de particulares.
  - México cuenta con un cuerpo normativo sólido en materia de protección de datos personales dentro del cual se destacan la Ley Federal de Transparencia y Acceso a la Información Pública y Gubernamental (en la cual se delimita la información reservada y confidencial y regula las solicitudes de liberación de información) y la Ley Federal de Protección de Datos en Posesión de los Particulares (que unifica por primera vez en el nivel federal obligaciones para compañías y entidades privadas que recolectan, procesan, almacenan o manejan datos personales).
  - Finalmente, se debe reconocer que el marco normativo mexicano alcanza en muchos sentidos los niveles de protección exigidos por la Unión Europea y si bien no ha sido reconocido como adecuado, la co-existencia de legislación estatal sobre la materia facilita la adopción por

los procesadores de datos, de medidas que superen incluso los mínimos federales de privacidad, refiriéndose a elementos que no han sido regulados específicamente, como lo son las *cookies* y las aplicaciones móviles.

- Japón
    - Caracterizado por contar con fundamentos puramente legales y por un sistema similar al de las directivas europeas (directrices del gobierno central que deben ser aplicadas por los gobiernos locales), el sistema legal japonés cuenta en materia de protección de datos personales con la Ley sobre Protección de Información Personal Número 57 de 2003, la cual ha sido complementada por más de dos mil directrices emitidas por gobiernos locales y municipalidades a la fecha.
    - Dicha ley se fundamenta en el hecho de que la información personal debe ser manejada cautelosamente con la filosofía de respeto al individuo, por lo que promueve el manejo adecuado de la información personal mediante el establecimiento de guías generales que servirán posteriormente como fundamento para la creación de reglas específicas por parte de los ministerios.
    - Dentro de sus elementos más característicos se puede encontrar tanto el hecho de que la ley asigna el papel de ente regulador a los diversos ministerios relevantes; como la inexistencia de disposiciones sobre temas como las transferencias internacionales de datos personales o el deber de notificar al interesado en caso de violaciones a sus datos personales. Por ello, el gobierno japonés se encuentra actualmente discutiendo la necesidad de actualizar o reformar esta normativa.
- China
    - Ejemplo de los países cuyo marco legal en materia de protección de datos es sumamente limitado (más no inexistente), el caso chino se caracteriza tanto por la inexistencia de una ley general como la inexistencia de un reconocimiento constitucional de la intimidad o la privacidad.

- Frente a las evidentes consecuencias de tan importante omisión, el gobierno chino ha procurado promulgar una serie de normas estatutarias dirigidas a tratar este problema, aunque sea indirectamente.
- Asimismo, en los últimos años han sido generados dos elementos legales que constituyen un primer paso hacia la regulación directa de la protección de datos personales: la Decisión sobre el fortalecimiento de la protección de la información en Internet (único de los dos con carácter vinculante) y las Guías para la protección de la información personal en sistemas de información para servicios públicos y comerciales.

## Sección III: Sistemas y Estándares Internacionales para la Protección de Datos

Habiendo estudiado una gran cantidad de las legislaciones nacionales y regionales que rigen la protección de datos en el mundo moderno, se podrá abarcar ahora el estudio de algunos de los sistemas que pretenden expandir dicha protección al ámbito internacional. No es este un tema fácil de estudiar, por supuesto; basta con dar una mirada a las pasadas dos secciones para comprender que el tema ha sido abarcado de maneras muy diversas a lo largo del globo (y con grandes variaciones en los niveles de protección reconocidos por cada sistema).

A pesar de lo anterior, los desafíos surgidos frente a la convergencia de las telecomunicaciones llaman de manera cada vez más imperiosa hacia la armonización legal de la protección de datos personales en el orbe. Para ello, algunos de los entes internacionales con mayor peso dentro del mundo de la protección de datos personales han planteado ya algunos fundamentos que apuntan finalmente hacia la creación de un sistema internacional unificado o, por lo menos, hacia la generación de sistemas interoperables que permitan la aplicación de las diversas disposiciones nacionales en el plano internacional.

Asimismo, se cuenta también en la actualidad con algunos ejemplos de estándares internacionales que buscan aportar algunas soluciones al problema desde el punto de vista técnico.

En tanto se busca brindar al lector un panorama amplio sobre la protección de datos en los diversos niveles que se relacionan con la convergencia de las

telecomunicaciones, se considera fundamental concluir el presente capítulo mediante el estudio de algunos de los sistemas internacionales existentes, así como de los estándares técnicos más relevantes para la presente investigación.

### *Sistemas Internacionales*

Tal como se mencionaba con anterioridad, actualmente resulta imposible identificar un marco de Derecho Internacional (salvo los fundamentos encontrados en los institutos de derechos humanos ya estudiados) aplicable a todos los países del mundo. Tomando esta afirmación como base, puede afirmarse que nos encontramos en un momento histórico difícil para la protección de datos personales en tanto incluso son contados los ejemplos de tratados internacionales que se relacionan directamente con la materia.

A pesar de lo anterior, existen ejemplos claros de sistemas internacionales que procuran brindar bases legales que posibiliten el ejercicio del derecho fundamental a la autodeterminación informativa en el ámbito internacional y que brindan esperanza al recordar la posibilidad de llegar algún día a contar con un *tratado internacional universal* sobre estos temas (o incluso a la *telecivitas o gobierno del ciberespacio,* para la regulación de las redes globales de telecomunicaciones y singularmente del internet, a la que hacía referencia Suñé Llinás (Suñé Llinás, 2006, págs. 318-319)).

Así, existen en la actualidad algunos sistemas que han surgido a partir de modelos regionales y que han sido extendidos en el plano internacional para admitir situaciones especiales o para reconocer su interoperabilidad con otros marcos legales (modelo Europeo ya estudiado) y el programa de Safe Harbor aplicado en Estados Unidos; así como su reconocimiento de la “protección adecuada” brindada por países ajenos a la

Unión Europea. Por otro lado, existen algunos ejemplos de sistemas establecidos por entes internacionales que procuran sentar las bases para la futura construcción de un modelo internacional más estable (APEC, Naciones Unidas y OCDE).

A continuación se examinará con mayor detalle cada uno de estos sistemas.

### Convenio 108 del Consejo de Europa del 28 de Enero de 1981 para la Protección de los Individuos con Respecto al Procesamiento Automatizado de Datos Personales de 1980 y su Protocolo Adicional de 2001

Ya estudiado en la primera sección del presente capítulo, este convenio no solamente se caracteriza por su rigurosidad y por formar parte del marco fundamental de la Protección de Datos en la Unión Europea, sino que se constituye en el único instrumento legal internacional vigente en materia de protección de datos personales que posee un ámbito de aplicación mundial y se encuentra abierto a ser firmado y ratificado por cualquier país del mundo (Electronic Privacy Information Center, 2013).

### El Programa de Safe Harbor

Creado a finales de la década de 1990, el programa de Safe Harbor (o Bahía Segura), es una respuesta a la difícil realidad que, para Estados Unidos de América resultó a partir de la adopción, por parte de la Unión Europea, la Directiva 95/46/EC. Tal como se estudió con anterioridad, las disposiciones de la Directiva en materia de transferencia

internacional de datos personales establecían claramente la prohibición de realizar dichas transferencias a aquellos países que no contaran con un nivel adecuado de protección.

Como se pudo observar a partir del análisis legislativo anteriormente realizado, Estados Unidos no cuenta actualmente (ni mucho menos durante finales de los años noventa) con una legislación robusta y seria que regule de manera vinculante el tema de la protección de datos personales, sino que se basa fundamentalmente en un sistema de autorregulación para el sector privado y de regulación mínima para el sector público (con extensas excepciones aplicables en nombre de la seguridad nacional, las cuales no han hecho otra cosa más que aumentar a partir de la promulgación de la PATRIOT Act.).

Ante esta realidad la posibilidad de que los países de la Unión Europea reconocieran como adecuado el nivel de protección brindado por EEUU a los datos de sus ciudadanos era prácticamente nulo. Esta situación preocupó seriamente tanto a los países miembros de la Unión como al gobierno de los Estados Unidos de América, en tanto ambas potencias mantienen estrechos vínculos comerciales que podrían verse afectados seriamente por la implementación a destajo de la Directiva 95/46/EC.

La polémica generada durante dicha época llevó finalmente a un acercamiento del Departamento de Comercio estadounidense con la Comisión Europea y representantes de la industria, el cual finalmente llevó a la generación del programa de Safe Harbor como solución al problema. De esta manera, para el año 2000 las medidas adoptadas por medio del programa de Safe Harbor fueron reconocidas por la Unión Europea

como protección adecuada para los datos personales (Comisión Europea, 2000) y han mantenido su vigencia desde la fecha.

Puesto de una manera sencilla, el programa de Safe Harbor es un sistema de cooperación que permite a las empresas y organizaciones interesadas en exportar e importar datos personales de la Unión Europea, autocertificar que cumplen con las disposiciones de la Directiva 95/46/CE (con el deber de renovar tal certificado anualmente), creando de esta manera un sistema más flexible que permite superar las limitaciones legales del contexto estadounidense.

A la hora de estudiar el programa de Safe Harbor se debe comenzar por establecer que este sistema prevé la posibilidad de que las organizaciones certifiquen su nivel de protección respecto a ciertas categorías específicas de datos personales (situación relativamente común en la práctica). Dicha autocertificación se encontrará basada fundamentalmente en seis requisitos, a saber:

- El desarrollo e implementación de un manifiesto de privacidad bajo las disposiciones del programa de Safe Harbor.
- La publicación de dicho manifiesto.
- La designación de un oficial de protección de datos.
- El establecimiento de un programa de entrenamiento para sus empleados.
- El establecer un mecanismo de verificación para auditar el cumplimiento de la compañía con los principios.
- El establecimiento de un mecanismo independiente de resolución de disputas.

En términos generales, el manifiesto que deberán adoptar las organizaciones interesadas en formar parte del programa de Safe Harbor, deben asumir políticas que cumplan con las disposiciones de la Directiva 95/46/EC. Así, se puede resumir como fundamental dentro de este conjunto de obligaciones la adopción de siete principios de la protección de datos personales, a saber:

- Principio de notificación
    - La compañía debe informar al individuo sobre el tipo de información recolectada, el propósito de la recolección, la manera en que será usada la información, cómo contactar a la organización con consultas o quejas, los tipos de terceros interesados a los que podrá revelar la información, las opciones y medios que ofrece la organización a los individuos para limitar el uso y revelación de la información y cómo será asegurada la información.
- Principio de elección
    - Debe darse a escoger al individuo si sus datos podrán ser publicados a terceras partes o usados para propósitos no compatibles con los propósitos originales, (en este caso la elección puede ser del tipo opt-out[190]; si los datos son sensibles el mecanismo debe ser opt-in[191]).
- Principios relacionados con las transferencias de datos
    - La compañía puede transferir datos a un no agente solo si le ha notificado al sujeto de datos la transferencia y la oportunidad de hacer opt-out o opt-in, según corresponda

[190] Optar para salir, método comúnmente utilizado en los contratos y declaraciones de condiciones de uso en Internet mediante el cual se agrega automáticamente al usuario dentro de ciertas políticas y se presupone su consentimiento, quedando a su voluntad el solicitar se le excluya de dichas prácticas.
[191] Optar para entrar, el opuesto del Opt-Out.

- La compañía puede transferir datos a un agente de un tercer interesado si el agente está dentro de la Unión Europea, el agente se encuentra incluido en el programa de Safe Harbor, o si por medios contractuales se asegura la adecuación de la tercera parte.
- La compañía no es responsable del mal uso dado por el tercer agente si ha cumplido con los requisitos, a menos de que la organización supiera o debiera saber que habría mal uso y no se hizo nada al respecto.

- Principio de Seguridad
  - Deber tomar precauciones razonables para proteger los datos personales de pérdida, mal uso, acceso sin autorización, publicación, alteración y destrucción.
- Principio de Integridad de los datos
    - Los datos solamente podrán ser recolectados para propósitos específicos; la información deberá ser relevante y su uso solo podrá darse para propósitos no incompatibles para los propósitos de la recogida. Puede darse por nuevas autorizaciones brindadas por el interesado y siempre deben tomarse pasos razonables para asegurar que los datos sean confiables, veraces, completos y actuales.
- Principio de Acceso
  - Establece el deber de garantizar acceso a individuos y estos deben ser capaces de corregir, enmendar o borrar información no veraz.
    - Puede negarse dicho acceso si la organización demuestra que:

- La publicación puede interferir con la salvaguarda de intereses públicos como la seguridad nacional o pública.
- Interferir con usos policiales.
- Interferir con causas privadas de acción.
- Publicar información ajena.
- Romper un privilegio legal o profesional (u obligaciones).
- Romper la confidencialidad necesaria para negociaciones actuales o futuras.
- Afectar investigaciones de seguridad de empleados o procedimientos de quejas.
- Afectar confidencialidad en conexión con empleados y reorganizaciones.
- Afectar la confidencialidad necesaria para el monitoreo de la gerencia económica o financiera.
- El peso de la prueba de proveer acceso sería desproporcionado o los derechos legítimos de otros serían violados.

### Protección Adecuada Según Estándares Europeos

También parte del sistema europeo, la certificación de nivel adecuado de protección según estándares europeos se constituye actualmente en la principal manera de determinar si un país cuenta o no con un alto nivel de protección a los datos

personales de sus ciudadanos. Específicamente, la certificación de protección adecuada a los estándares europeos procura determinar que un Estado cuenta con un grado de protección superior, igual, similar, o equivalente al sostenido en la Unión Europea; esto con miras a *"evitar la creación de paraísos informáticos (data havens), es decir, jurisdicciones donde la carencia de leyes de protección de datos, las trasforme en sitios atractivos para realizar tratamientos de datos personales que puedan ser violatorios de otras leyes de privacidad"* (Remolina-Angarita, 2010, pág. 467).

En el caso de la certificación europea, se puede comprender, siguiendo al grupo de trabajo Artículo 29[192], que las formas de evaluar el nivel de protección de terceros países se basa tanto en factores de naturaleza regulatoria como de naturaleza instrumental e institucional, que incluyen tanto el contenido del marco legal y constitucional aplicable dentro de dicho país en materia de protección de datos personales como a la realidad de la aplicación de dicha normativa por medio de la existencia de elementos como un ente regulador independiente encargado de garantizar tal protección.

Finalmente, resulta necesario recalcar que, según Remolina-Angarita, para que la normativa de un tercer país sea considerada como adecuada, deberá contener como mínimo los siguientes principios básicos: *"Limitación de la finalidad; calidad de los datos y proporcionalidad; transparencia; seguridad; acceso, rectificación y oposición; Restricciones a las transferencias sucesivas a otros terceros países."* (Remolina-Angarita, 2010, pág. 501). Y, como aspectos adicionales aplicables a tipos especiales de tratamiento, deberán

[192] Grupo de trabajo constituido por representantes de cada uno de las agencias de protección de datos de los Estados Miembros de la Unión Europea. Sus materiales y opiniones pueden ser encontrados en (Comisión Europea, 2014).

contener disposiciones en materia de *"Datos sensibles; mercadeo directo; decisión individual automatizada"* (Remolina-Angarita, 2010, pág. 501).

## Guías de la Organización para la Cooperación y el Desarrollo Económico

Adoptadas en Septiembre de 1980, la Guía de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales (Organización para la Cooperación y el Desarrollo Económico, 1980) constituye actualmente un referente necesario en todo estudio sobre el tema, en tanto sus disposiciones fueron el primer ejemplo de principios aceptados internacionalmente en materia de protección de datos personales.

Caracterizada por establecer uno de los primeros marcos de principios y políticas relacionados con los niveles operacionales del tratamiento de datos personales, la Guía ha sido base de gran cantidad de legislaciones y reglamentos relacionados con la materia y sus disposiciones han sido adoptadas y replicadas por países como Estados Unidos, Canadá, Alemania, Suiza, Australia, Nueva Zelanda y la Unión Europea.

El conjunto de "Prácticas Justas de la Información"[193] planteadas por la Guía procuran fundamentalmente el potenciamiento de una cultura de seguridad por ser compartida internacionalmente en los albores de la Sociedad de la Información y la Comunicación; para lo cual la redacción original del documento de 1980 se preocupaba básicamente por definir los temas tratados, establecer los principios básicos (por ser aplicados tanto

[193] Término general que comprende un conjunto de estándares dirigidos a gobernar la recolección y uso de los datos personales.

nacional como internacionalmente) y delimitar algunos de los fundamentos relacionados con la implementación de los principios en el nivel nacional e internacional por sus Estados miembros.

De esta manera, la OCDE estableció desde 1980, un conjunto de ocho principios básicos que debían ser aplicados en el nivel nacional (Organización para la Cooperación y el Desarrollo Económico, 1980), a saber[194]:

1) Principio de Limitación de la Recolección.
2) Principio de Calidad de los Datos.
3) Principio de Especificación de los Propósitos.
4) Principio de Limitación de los Usos.
5) Principio de Salvaguardas en Seguridad.
6) Principio de Apertura.
7) Principio de Participación Individual.
8) Principio de Responsabilidad.

De esta misma manera, los principios admitidos por la OCDE como de aplicación internacional fueron los siguientes:

1) Principio de Libre Circulación de la Información.
2) Principio de Restricción Legítima.

Tal como se señaló con anterioridad, una vez establecidos dichos principios, la Guía de la OCDE se preocupa por establecer la manera por medio de la cual estos serán aplicados en nivel nacional e internacional. Para tal fin, establece que, en el nivel

[194] El contenido de los cuales ya ha sido abordado ampliamente a lo largo del presente trabajo, específicamente en la sección primera del segundo capítulo

nacional, los Estados miembros habrán de considerar las implicaciones del procesamiento y la reexportación de los datos personales; tomar todos los pasos razonables y apropiados para asegurar que los flujos transfronterizos de datos que transiten por su territorio sean ininterrumpidos y seguros; abstenerse de restringir los flujos transfronterizos de datos personales entre su territorio y el territorio de otro Estado miembro (siempre que este observe esta Guía); y evitar crear leyes, políticas y prácticas que limiten u obstaculicen los flujos transfronterizos de datos.

En el nivel internacional, la Guía establece básicamente un sistema de cooperación que requiere de sus Estados miembros el publicar a otros Estados miembros sus detalles en materia de observancia a los principios establecidos en la Guía; asegurar la simplicidad y compatibilidad de sus trámites en materia de flujos transfronterizos de datos y protección de datos personales con los de otros países miembros; establecer procedimientos para intercambiar información y ofrecer asistencia mutua entre los Estados miembros, y trabajar hacia el desarrollo de principios nacionales e internacionales que gobiernen las leyes aplicables a los flujos transfronterizos de datos.

Durante la década de 1990 y de 2000, la OCDE se dio a la tarea de monitorear la aplicación de los principios por los diversos Estados miembros y a formar grupos de trabajo dirigidos a fomentar la educación, combatir el cibercrimen y desarrollar equipos de respuesta a incidentes de seguridad de la información; sin embargo, para finales de la década de 2000 resultaba evidente que era necesario realizar una actualización a la Guía y a sus anexos, por lo cual en 2013 la OCDE creó un grupo de múltiples interesados que sería encargado de tal tarea.

En su versión de 2013, la Guía mantiene sus elementos fundamentales, pero ha visto actualizado su enfoque práctico al adoptar una visión coordinada de las estrategias nacionales de protección de datos que contemplen el manejo de riesgos (prevención en lugar de reparación). Por otra parte, la nueva edición de la guía procura la búsqueda de interoperabilidad en los esfuerzos internacionales.

Finalmente, se debe recalcar que esta revisión agrega una importante sección dirigida en su totalidad a regular la manera en que deberá ser implementado el principio de responsabilidad, por parte de los controladores de datos[195]. De esta manera se encontrará a lo largo de la sección cuarta de la Guía, que se requiere de todo controlador el poseer un programa de manejo de la privacidad[196]; encontrarse preparado para demostrar ante entes responsables su adecuado manejo de los datos personales; y realizar notificaciones apropiadas a las autoridades relevantes y a los interesados cuando se den violaciones a los datos bajo su custodia (Organización para la Cooperación y el Desarrollo Económico, 2013).

### Red Iberoamericana de Protección de Datos

Patrocinada por la Agencia Española de Protección de Datos, la Red Iberoamericana de Protección de Datos reúne a 22 países de la región Iberoamericana (incluyendo a Costa

[195] Públicos y privados por extensión de la obligación de los Estados miembros de adoptar estos principios dentro de su marco normativo
[196] Que implemente las Prácticas Justas de la Información de acuerdo con las características de la empresa y sus operaciones frente a un adecuado estudio de riesgos; sea integrado dentro de su estructura interna y en sus procesos de auditoría y sea capaz de responder a incidentes eventuales

Rica) en un foro multilateral dirigido a la armonización de la legislación nacional sobre la materia con base en las disposiciones de la directiva Europea 95/46/CE.

A lo largo de sus 12 años de funcionamiento, la Red Iberoamericana de Protección de Datos ha generado una gran cantidad de acuerdos y convenios que reúnen la voluntad de participación en esta iniciativa de múltiples organizaciones observadoras y, por supuesto, de los diversos países miembros. Asimismo, a lo largo de sus encuentros, la Red ha generado un buen número de declaraciones, en las cuales han acordado:

- 2002 – la promoción de un intercambio continuo y fluido de información, procurar un nivel adecuado de protección de datos personales y establecer un foro permanente dirigido a coordinar estas actuaciones (Red Iberoamericana de Protección de Datos, 2002).
- 2003 – reforzar los esfuerzos acordados así como la cooperación mutua y continua y procurar el establecimiento de canales de diálogo (Red Iberoamericana de Protección de Datos, 2003).
- 2004 – examinan temas como la protección de datos y la perspectiva del sector financiero; la lucha contra el SPAM; las transferencias internacionales de datos; las reacciones del sector telecomunicaciones e internet ante los ataques a la privacidad y el sector comercial y el uso de la información con fines de marketing. A partir de lo cual acuerdan la creación de subgrupos de trabajo, actualización periódica y la organización de una secretaría “pro tempore” (Red Iberoamericana de Protección de Datos, 2004).

- 2005 – examinan entre otros temas el derecho fundamental a la protección de los datos personales, las nuevas tecnologías de la información, los desenvolvimientos normativos globales, la necesidad de asegurar especialmente los datos de salud y acuerdan tanto la cooperación entre varias de las instituciones participantes como la ampliación de los subgrupos de trabajo (Red Iberoamericana de Protección de Datos, 2005).
- 2007 – examina los flujos internacionales de datos en ensayos clínicos y la investigación biomédica y el tratamiento de los datos personales de menores en internet, por lo que se promueve una iniciativa para analizar esta realidad y adoptar medidas prácticas. Asimismo fueron aprobadas las "Directivas de Armonización de Protección de Datos en la Comunidad Iberoamericana" [197] (Red Iberoamericana de Protección de Datos Personales, 2007).
- 2008 – se logran acuerdos sobre los principios necesarios para el tratamiento de los datos personales: lealtad, licitud, decisión personal, educación, especificidad, finalidad, exactitud y veracidad, protección a categorías especiales, confidencialidad y seguridad de la información, información, rectificación, cancelación y oposición, legalidad y efectividad. (Red Iberoamericanda de Protección de Datos, 2008).
- 2009 – se declara conjuntamente con la Asociación Francófona de Autoridades de Protección de Datos Personales la voluntad de cooperación internacional y el apoyo al desarrollo de instrumentos internacionales, entre otros temas (Red Iberoamericana de Protección de Datos, 2009).

[197] Disponibles en (Red Iberoamericana de Protección de Datos, 2007).

- 2010 – los miembros de la red acuerdan impulsar la promulgación de leyes en un nivel local, la promoción de las autoridades garantes de este derecho, la sensibilización a la población, la mejora de las prácticas de gestión de datos y la adopción de estándares regionales e internacionales, entre otros temas (Red Iberoamericana de Protección de Datos, 2010).
- 2011 –asumen los acuerdos de dialogar, discutir y analizar los diversos problemas existentes; compartir información con las nuevas autoridades, asegurar que dicho diálogo no comprometa la independencia de las autoridades de protección de datos, exponer y discutir los avances logrados en la 34ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos (Red Iberoamericana de Protección de Datos, 2011).
- 2012 – a raíz de la cual se fortalecen los trabajos de la red para la cooperación y participación de sus miembros, así como de los mecanismos de cooperación internacional. También se acuerda promover la normativa sobre el tema y dar continuidad a los trabajos de creación de herramientas de consulta jurisprudencial para la región (Red Iberoamericana de Protección de Datos, 2012).
- 2013 – por la que sus miembros concuerdan en la necesidad de impulsar el fortalecimiento institucional de la red, intensificar el diálogo, garantizar el buen uso de los datos transferidos en los niveles local e internacional, incrementar la cooperación entre las autoridades relevantes, cooperar con la OEA para impulsar proyectos sobre el tema y dar continuidad a los trabajos generados en encuentros pasados (Red Iberoamericana de Protección de Datos, 2013).

### Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico

El Fondo de Cooperación Económica Asia-Pacífico (APEC) es un foro multilateral creado en 1989 para considerar el crecimiento y prosperidad de los países del Pacífico mediante su cooperación en diversas áreas. Como parte de estas metas, y como manera de fomentar el comercio electrónico, en 2005 el foro aprobó su *Marco de Privacidad,* mediante el cual se intenta establecer un conjunto de principios fundamentales en materia de privacidad y protección de datos personales que logren coordinar estos temas entre los países miembros.

La principal característica del Marco de Privacidad de la APEC es su flexibilidad. El marco reconoce la necesaria transmisión transfronteriza de datos en el mundo moderno, así como la existencia de multiplicidad de sistemas de protección de datos personales que brindan diversos niveles de protección a los individuos.

Ante esta situación el Marco procura *"favorecer sistemas de protección que prevengan la restricción innecesaria del flujo de datos, balanceando la necesidad de protección con los intereses comerciales y las necesidades corporativas y el necesario reconocimiento a las diversidades de los países miembros" (Foro de Cooperación Económica Asia-Pacífico, 2005, pág. 3).*

Para lograr tal fin el Marco establece nueve principios acordes con los principios establecidos en 1980 por la OCDE, que se caracterizan fundamentalmente por buscar la interoperabilidad y la responsabilidad en el tratamiento de los datos personales y los

sistemas de protección de datos personales aplicados en los diversos países. Para ello, la APEC ha fomentado la adopción de autorregulación vinculante[198] en las compañías, que puede ser certificada por terceras partes y las autoridades reguladoras de los países miembros.

Básicamente, los principios establecidos por el Marco de Privacidad (Foro de Cooperación Económica Asia-Pacífico, 2005, págs. 11-29) son:

- La prevención del daño: reconociendo los intereses del individuo, procura el diseño de los sistemas y medidas de protección de datos personales para prevenir el mal uso de la información y la implementación de medidas de remedio en caso de que tales situaciones se den. Estas medidas deberán ser aplicadas tanto por entes públicos como privados, en proporción a la severidad del daño potencial.
- Notificación: Los controladores de datos personales deberán publicar sus políticas sobre la materia de forma clara y accesible, incluyendo en ellas explicaciones sobre el hecho de que se están recolectando datos personales[199]; los propósitos de la recolección; los tipos de personas u organizaciones con los que se comparte dicha información; la identidad y localización del controlador de datos (y su información de contacto); y las opciones disponibles para los individuos que deseen limitar el tratamiento de su información.
- Limitaciones a la recolección de datos: Establecidas de acuerdo con la relevancia de la información y entendiéndose que dicha recolección debe darse de manera legal y justa, con notificación y consentimiento del interesado.

[198] Sobre el tema ver también (Foro de Cooperación Económica Asia-Pacífico, 2005).
[199] Pese a lo cual reconoce el Marco que existen casos en los que este principio puede no ser completamente aplicable, como por ejemplo en el caso de que se recolecte información pública o provista por terceros.

- Usos de la información personal: Establece este principio que la información recopilada solamente debe servir para los fines de su recolección y aquellos relacionados o compatibles con estos, excepto cuando se cuente con consentimiento del interesado, cuando sea necesario por ley o para proveer un servicio o producto solicitado por el individuo.
- Elección: Cuando sea apropiado, debe facilitarse a los individuos métodos claros, prominentes, fácilmente comprensibles, accesibles y asequibles para disponer sobre la recolección, uso y publicación de sus datos personales[200].
- Integridad de la Información personal: Procura asegurar que la información sea exacta, completa y actualizada según los propósitos del uso.
- Salvaguardas de la Información: Requiere que los controladores de información personal protejan adecuadamente la información en su poder frente al acceso, destrucción, uso, modificación o publicación sin autorización de esta; son utilizadas para este fin salvaguardas [201] proporcionales, los daños potenciales y a la sensibilidad de la información.
- Acceso y corrección: Procura asegurar estos derechos a los individuos, para lo cual requiere que se les permita obtener confirmación de si se manejan datos sobre ellos y requerir que esta les sea facilitada[202] de manera expedita, barata, razonable

[200] Con independencia de si estos métodos son facilitados de manera física o digital. Se establece también que el requisito de que estos sean "fácilmente comprensibles" solamente será aplicable entre los países miembros de la APEC. Finalmente, también se reconoce la posibilidad de que se den situaciones en las cuales el consentimiento se obtenga implícitamente o en las cuales no sea necesario proveer dichos mecanismos.
[201] Revisadas y actualizadas periódicamente.
[202] Previa comprobación fidedigna de su identidad.

y comprensible y, en caso de que sea necesario, puedan solicitar que esta sea rectificada, completada, enmendada o borrada[203].

- Responsabilidad: Establece que todo controlador de datos personales debe ser responsable por el cumplimiento de las medidas que lleven estos principios a la realidad; asimismo será responsable de asegurarse de cumplir con su debida diligencia y de obtener el consentimiento del usuario cuando la información personal sea transferida nacional o internacionalmente, así como de asegurarse de que el receptor de dicha información cumplirá también con las disposiciones de estos principios.

Finalmente, el Marco de Privacidad de la APEC establece algunas guías para la implementación de los principios tanto en el ámbito nacional como el internacional. En el nacional establece básicamente la necesidad de que los países tomen en consideración que: *"Reconociendo los intereses de las economías en la maximización de los beneficios económicos y sociales disponibles para sus ciudadanos y negocios, la información personal debe ser recolectada, almacenada, procesada, utilizada, transferida y publicada de maneras que protejan la privacidad de la información individual y les permita a los individuos darse cuenta de los beneficios de los flujos de información dentro y fuera de las fronteras"* (Foro de Cooperación Económica Asia-Pacífico, 2005, pág. 30).

Asimismo, se establece como guía para resolver las discrepancias en temas específicos la búsqueda de la máxima compatibilidad entre las medidas adoptadas por los países miembros. Y si bien la APEC no menciona los medios específicos por los cuales los

[203] Excepto en caso de que el costo de hacerlo fuera irrazonable o desproporcionado; cuando la información no pudiera ser liberada por motivos legales, se seguridad o para proteger información comercial; y cuando se pudiera afectar la privacidad de terceros. Siempre debe brindarse al individuo respuesta razonada en caso de no concederse su solicitud.

Estados miembros habrán de llevar a cabo dichos principios, los incentiva a adoptar prácticas no discriminatorias mediante la discusión de las medidas por ser tomadas entre los diversos grupos de interesados (públicos y privados) y una fuerte campaña de educación en el nivel interno.

Precisamente con en materia de cooperación entre ambos sectores la APEC establece que: *"La participación activa de entidades no gubernamentales ayudará a asegurar que todos los beneficios del Marco de Privacidad de la APEC puedan ser realizados. De acuerdo con esto, las Economías Miembro deberán entablar diálogos con los sectores privados relevantes, incluyendo a los grupos de privacidad y a aquellos que representen a los consumidores y a la industria, para obtener su opinión en materias relacionadas con la protección de la privacidad y la cooperación en el mejoramiento de los objetivos del Marco. Más aún, especialmente en las economías en las que no se han establecido regímenes de protección a la privacidad en su jurisdicción doméstica, las Economías Miembro deberán dedicar amplia atención a reflejar las opiniones del sector privado en el desarrollo de protecciones a la privacidad. En particular, las Economías miembro deberán buscar la cooperación de entidades no gubernamentales en la educación pública y fomentar el que estas refieran sus quejas a las agencias de protección de la privacidad así como a asegurar su cooperación continuada en la investigación de dichas quejas"* (Foro de Cooperación Económica Asia-Pacífico, 2005, pág. 32).

En ámbito internacional, la APEC establece la necesidad de compartir información entre las *economías miembros* y educarse entre sí en materia de protección de datos (compartiendo programas de entrenamiento y otros) a la vez que deberán publicar a las demás sus respectivas autoridades encargadas de llevar a cabo dichas tareas. Por otra parte, se exige de los Estados miembros una mayor cooperación transfronteriza en la investigación y ejecución de las protecciones a los datos personales, fomentando

los acuerdos bilaterales y multilaterales de conformidad con las posibilidades de la ley[204].

Precisamente el Marco concluye estableciendo bases en materia de generación de normativa internacional, para lo cual establece la necesidad de desarrollo y reconocimiento de las reglas transfronterizas[205] de las diversas organizaciones y empresas; así como la necesidad de estas de acoplarse siempre a las disposiciones de las leyes locales. Para ello incentiva a todos los países miembros a trabajar junto con los actores interesados relevantes y con sus pares internacionales, para generar marcos o mecanismos para el reconocimiento mutuo o aceptación de las reglas transfronterizas de protección de datos y la generación de reglas sobre el tema, que faciliten la transmisión internacional de datos de manera responsable sin crear barreras innecesarias a los flujos de información.

### Resoluciones y Declaraciones de las Conferencias Internacionales de Autoridades de Protección de Datos y Privacidad

Establecida en 1979 y celebrada anualmente, la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad es actualmente el mayor foro dedicado a la regulación armoniosa de la materia en el ámbito mundial. Estas conferencias reúnen a las más altas autoridades e instituciones relacionadas con la

[204] Estableciendo la posibilidad de crear mecanismos de notificación expedita, mecanismos de asistencia a la investigación y dirigidos a compartir información o a dar mayor prioridad a algunos casos según la severidad de los daños potenciales, así como el tomar pasos para fomentar la confidencialidad de la información intercambiada para todos estos fines.
[205] Auto-regulación vinculante basada en los principios del Marco.

protección de datos personales del mundo, quienes (junto con expertos en las diversas materias) generan resoluciones y declaraciones dirigidas a guiar a los países en la solución de los problemas que estos enfrentan.

Precisamente, dado que estas conferencias son llevadas a cabo una vez al año, el contenido de sus resoluciones ha sido especialmente variado; sin embargo, se puede resaltar la importancia de algunas de ellas para el tema en estudio, como por ejemplo:

Declaración de Varsovia sobre la "Appification" de la Sociedad – La Privacidad: una Brújula para un Mundo en Turbulencia

> En ella se reconoce la importancia de la convergencia de las telecomunicaciones y los dispositivos móviles en nuestra sociedad, a la vez que se acepta el rol cada vez más importante que toman las aplicaciones en los nuevos dispositivos. Con base en este reconocimiento se propone fomentar el control de los usuarios de aplicaciones móviles y la necesidad de que las aplicaciones sean creadas de conformidad con el principio de *"disminuir la aparición de sorpresas para el usuario: excluir características o propiedades ocultas, no recabar datos sin especificar el contexto del acopio"* (Autoridades Internacionales de Protección de Datos y Privacidad, 2013, pág. 2).
>
> Asimismo, se reconoce la gran responsabilidad que recae tanto en los desarrolladores de las aplicaciones como en los proveedores de sistemas operativos en el crecimiento de la economía digital, por lo que deben asumir un papel responsable e incluir la privacidad por diseño como parte de sus

programas; por ejemplo, asegurándose de que ningún programa o plug-in[206] utilizado recopile información sin consentimiento del usuario o, en el caso de la industria, mediante la generación de sellos, certificados de calidad y otros esquemas de autorregulación vinculante (Autoridades Internacionales de Protección de Datos y Privacidad, 2013).

### Resolución sobre el Futuro de la Privacidad

En la que, partiendo de las realidad y de las discusiones sobre la necesidad de realizar cambios a los sistemas legales que imperaron durante las décadas pasadas en materia de protección de datos personales, se decide que los miembros deberán intensificar su cooperación con miras a responder a los riesgos transfronterizos de la protección de datos de manera coordinada; compartir información y experiencia en lo posible, para asegurar la mejor utilización de los recursos escasos; y aprovechar los esfuerzos de reforma para asegurar la mayor interoperabilidad de los sistemas legales resultantes (Autoridades Internacionales de Protección de Datos y Privacidad, 2012).

### Resolución sobre la Computación en la Nube

En ella se acepta el interés creciente por la computación en la nube y al tiempo se aceptan las cada vez mayores y más válidas preocupaciones generadas por dichas tecnologías. Por ello se recomienda que la computación en la nube no

[206] Códigos creados por terceras partes que son utilizados normalmente para incorporar mayores funcionalidades a un programa informático, como por ejemplo la reproducción de video o la presentación de anuncios al usuario.

reduzca los estándares de protección de datos en comparación con los implementados en otros sistemas; que los controladores de datos lleven a cabo los análisis de riesgo necesarios antes de montar sus plataformas en la Nube; que se asegure adecuada transparencia, seguridad, responsabilidad y confianza en dichas plataformas; que se aumenten los esfuerzos de investigación en materia de estandarización, certificación por terceros y privacidad por diseño en la computación en la nube; se revise la adecuación de las legislaciones nacionales frente a los dilemas transfronterizos generados por estas tecnologías; y se facilite información y cooperación por los entes reguladores en estos temas.

### Declaración de Uruguay sobre la Creación de Perfiles

En la que, basándose en el tangible aumento de las informaciones personales que están siendo recopiladas y procesadas por sectores públicos y privados del mundo, se recomienda asegurar la transparencia de las operaciones de *big data* y generar confianza del público en los métodos utilizados; distinguir las operaciones de procesamiento conforme con tres fases[207]; verificar la validación continua de los perfiles generados y el mejoramiento de los algoritmos utilizados; asegurar que las operaciones de generación de perfiles no se lleven a cabo sin intervención humana; asegurar que las tareas de generación de perfiles y aplicación de estos no recaigan en el mismo ente;

[207] A saber: a) determinar cuál es la necesidad que justifica el procesamiento, b) decidir qué datos serán utilizados, y c) decidir de qué manera estas prácticas podrán ser implementadas en la práctica. (Estas tres etapas deberán ser reguladas y revisadas independientemente de ser posible)

asegurar la capacidad de los individuos de enfrentarse a los resultados de los perfiles que les incumba; asegurar que estas actividades solo se lleven a cabo si se cuenta con autoridades regulatorias fuertes e independientes, capaces de vigilar a ambos sectores y suficientemente informadas como para llevar a la práctica su vigilancia; y finalmente, asegurar que las agencias o autoridades regulatorias sean capaces de contradecir, supervisar y auditar las propuestas normativas que regulen las bases de datos públicas de manera firme e independiente (Autoridades Internacionales de Protección de Datos y Privacidad, 2012).

### Resolución sobre Privacidad por Diseño

En la que se reconoce la necesidad de implementar los principios y la supervisión de la protección de los datos personales desde las primeras etapas de la creación de nuevas tecnologías, así como en la operación y administración de estas y a lo largo de todo el ciclo de vida de la información.

Por lo anterior, se aprueba el reconocimiento de la privacidad por diseño como parte fundamental de la protección de datos personales; se fomenta la adopción de sus principios[208] y se invita a las autoridades competentes a promover la incorporación de los principios y políticas relacionadas con la

[208] Los principios son: 1) Proactivo no es reactivo; prevención, no remedio; 2) Privacidad por defecto; 3) Privacidad incorporada dentro del diseño; 4) Total funcionalidad: 5) Suma positiva, no suma cero; 6) Protección de inicio a fin del ciclo de vida de la información; 7) Visibilidad y transparencia; 8) respeto a la privacidad del usuario.

privacidad por diseño de manera proactiva en sus respectivos países (Autoridades Internacionales de Protección de Datos y Privacidad, 2010).

### Resolución de Madrid sobre Estándares Internacionales para la Protección de los Datos Personales y la Privacidad

En la cual se realiza una propuesta conjunta para el establecimiento de un conjunto de principios internacionales para la protección de los datos personales y la privacidad de los usuarios[209], a la vez que se incorporan provisiones sobre los datos sensibles, los servicios de procesamiento, las transferencias internacionales, los derechos de los sujetos de datos, las medidas de seguridad y confidencialidad y disposiciones relevantes al cumplimiento y el monitoreo de estos principios de manera proactiva (Autoridades Internacionales de Protección de Datos y Privacidad, 2009).

### Propuesta de Resolución sobre Protección a la Privacidad en Redes Sociales

Que reconoce la popularidad de las redes sociales y su capacidad de facilitar perfiles autogenerados por los usuarios que permiten niveles nunca antes vistos de publicación de información personal, y dada la casi inexistente protección que existe en la actualidad, realiza recomendaciones tanto a los usuarios de redes sociales como a los proveedores de estas.

[209] Los principios propuestos son: Legalidad y justicia; especificación del fin; proporcionalidad; calidad de la información; apertura y responsabilidad.

Para los usuarios, la propuesta recomienda el uso cauto de estos servicios y la posibilidad de utilizar pseudónimos en lugar de su nombre real. Por su parte, a los proveedores la propuesta les recuerda sus responsabilidades; por ello, además de cumplir con sus responsabilidades con la Ley de Protección de Datos Personales vigente deberían seguir diez recomendaciones básicas; a saber: 1) el respeto de los estándares y normativas internacionales de protección de datos personales con independencia de la ubicación geográfica de sus servidores; 2) informar de manera transparente y abierta a sus usuarios sobre todo uso o tratamiento realizado a su información personal; 3) mejorar el control del usuario sobre su información personal y permitir las restricciones a la visibilidad de los perfiles de estos; 4) adoptar medidas por defecto que sean amigables con la privacidad del usuario; 5) mejorar y mantener siempre la seguridad de sus sistemas de información; 6) proveer a los individuos miembros y no miembros de la red social el derecho de acceso a aquellas informaciones suyas existentes en dicha red; 7) permitir el borrado fácil del perfil y la información relacionada; 8) permitir el uso de pseudónimos en los perfiles; 9) prevenir el acceso por terceros a la información de los perfiles sociales; y 10) permitir que la información de los perfiles sea indexada por buscadores de terceros solamente en los casos en los que la persona haya dado su autorización expresa (Autoridades Internacionales de Protección de Datos y Privacidad, 2008).

Resolución sobre el Proyecto de Norma ISO para la Privacidad

> Reconoció la necesidad de implementar mayores protecciones a la privacidad por medios técnicos y recomendó la creación de un estándar técnico de privacidad para ser desarrollado por la Organización Internacional para la Estandarización; este, habría de estar basado en las prácticas justas de la información, así como en los conceptos de escasez y minimización de los datos y anonimidad con miras a brindar criterios de evaluación y examen de los sistemas implementados por los diversos actores.
>
> Asimismo, esta resolución publica una serie de recomendaciones dirigidas a varios de los actores en el mundo de la estandarización internacional y específicamente dirigidas a la Organización Internacional para la Estandarización, con miras a expeditar y mejorar la creación de este nuevo estándar técnico (Autoridades Internacionales de Protección de Datos y Privacidad, 2004).

### *Soluciones Técnicas Internacionales*

Dado el enfoque iusinformático de la presente investigación, no se pueden dejar de lado en este estudio las soluciones técnicas con las que se cuenta en la actualidad para llevar a la práctica la protección de datos personales. Con esto en mente, seguidamente se centrará la atención en las posibles soluciones técnicas[210] que

[210] Que no pretenden ser una lista exhaustiva de las soluciones técnicas disponibles o posibles para la protección de datos en tanto estas surgen y evolucionan constantemente.

guardan gran relación con el tema en estudio: los RFC's de la IETF, los estándares ISO de la serie 27000; los estándares 29100 y 22307; dos de las soluciones técnicas más discutidas a lo largo de la última década: los protocolos P3P, *Do Not Track*; y se culminará este punto con un breve examen de la privacidad por diseño.

## Estándares Internacionales

Una de las mejores opciones con las que cuenta actualmente el mundo de la protección de datos personales frente al advenimiento de la convergencia tecnológica y el internet, puede ser encontrada en las soluciones técnicas. Adoptadas tanto en el nivel nacional[211] como el internacional, estas soluciones se deben a los procesos de estandarización coordinados por entes como el Grupo de Trabajo de Ingeniería de Internet (IETF por sus siglas en inglés), la Organización Internacional para la Estandarización, (ISO por sus siglas en inglés), la Unión Internacional de las Telecomunicaciones[212] (ITU por sus siglas en inglés) y otros.

Según ISO, *"un estándar es un documento que provee requisitos, especificaciones, guías o características que pueden ser utilizados consistentemente para asegurar que materiales, productos, procesos y servicios sean adecuados para sus propósitos (…) los estándares*

[211] Por medio de la adopción del estándar internacional como parte de la normativa técnica vinculante en el país o la creación de estándares nacionales que siguen de cerca las disposiciones del estándar internacional.

[212] Organización tristemente reconocida en los últimos años por la adopción de estándares que han socavado la autodeterminación informativa en las redes de nueva generación. Podemos encontrar un ejemplo de esta situación en el caso de la aprobación de la recomendación Y.2770 "Requisitos para la inspección profunda de paquetes en redes de nueva generación" en noviembre de 2012 que provocó serias críticas dadas sus serias implicaciones para la privacidad y la autodeterminación informativa de los usuarios finales.

*internacionales aseguran que los productos y servicios sean seguros, confiables y de buena calidad. Para las empresas, son herramientas estratégicas que reducen los costos al minimizar los desperdicios y los errores a la vez que incrementan la productividad. Ayudan a que las compañías atraigan nuevos mercados, nivelan el campo de juego para los países en desarrollo y facilitan el comercio libre y justo en el mundo" (International Standards Organization, 2013)*.

Tal como lo manifiesta ISO, los estándares internacionales poseen el potencial de ser aplicados ampliamente por la industria y el sector público por igual; asimismo, estos presentan ventajas atractivas que pueden impulsar su implementación por los diversos actores y grupos de interesados.

Ante este panorama, resulta indudable que los estándares internacionales relacionados con la seguridad de la información y el manejo de la privacidad y los datos de los individuos, adquieren relevancia para la presente investigación; por ello, a continuación se dedicará algún tiempo a su estudio.

### *RFCs de la Internet Engineering Task Force*

La Internet Engineering Task Force es uno de los entes internacionales más relevantes en la administración técnica del internet. Relacionada directamente con la Sociedad del Internet y otros entes de gobernanza por múltiples interesados, la IETF ha sido conocida por importantes contribuciones a lo largo de la historia del internet.

Con miras a cumplir su rol como generador de estándares abiertos (que pueden ser adoptados por cualquier interesado de manera voluntaria[213]), la IETF produce documentos conocidos como "Request for Comments" o peticiones de comentarios, los cuales pueden detallar desde estándares para ser adoptados por la industria, hasta especificaciones técnicas y descripciones de mejores prácticas.

A la fecha la IETF ha producido una buena cantidad de RFCs relacionados con la protección de la privacidad en internet, dentro de los cuales se encuentran los siguientes:

- RFC 1422: Generado en 1993, este RFC demuestra la larga data del trabajo de la IETF en materia de privacidad, pues se relaciona con el mejoramiento de la privacidad para el correo electrónico por internet por medio del manejo de llaves de certificados electrónicos.
- RFC 2778: Documento que plantea servicios de presencia que permiten a un usuario de servicios de información y telecomunicaciones monitorear la disponibilidad de otro usuario y su disposición para establecer comunicaciones (el estado de una persona en una ventana de chat, por ejemplo). Ante esta posibilidad el documento cuenta también con una serie de precauciones técnicas para el manejo de la los datos de presencia.
- RFC 4079: Expandiendo la información brindada por el RFC 2778, el RFC 4079 describe un sistema que no solamente brinda información sobre la presencia de un usuario en la red, sino que también reporta la ubicación geográfica de

[213] Lastimosamente, nuestro país la fecha no cuenta con ninguna herramienta legal que incentive la adopción de los RFCs de la IETF en el país, sin embargo el avance de la tecnología y la inclusión de estos en los productos tecnológicos ha significado que poco a poco las compañías de nuestro país han ido incorporando estos estándares a sus sistemas.

este (tal como sucede en las ventanas de chat de Facebook en la actualidad). Establece este documento también una serie de precauciones técnicas para la comunicación de dicha información.

- RFC 4745: De suma importancia, este RFC detalla un formato de documento específico dirigido a expresar las preferencias de privacidad de un usuario respecto a datos específicos para una aplicación, relacionando para ello los aspectos ya tratados en materia de localización y autorización.
- RFC 2804: Documento técnico que detalla la posición oficial de la IETF con respecto a las escuchas telefónicas, con base en la cual se opone esta institución a facilitar dentro de sus estándares los medios para falsear las comunicaciones electrónicas.
- RFC 6973: Documento fundamental para el futuro de la estandarización de la protección de datos personales; este RFC se titula "Consideraciones de privacidad para los protocolos de internet" y, si bien no constituye un estándar por sí mismo, sí contribuye a la información de la comunidad que crea estos estándares. Este documento reconoce los peligros de la seguridad y la privacidad, los métodos para mitigar estos peligros y finalmente establece algunas guías que buscan dirigir a la comunidad en el futuro.

Tal como se puede observar, los RFCs de la IETF constituyen documentos que tratan una gran cantidad de temas de variado nivel de complejidad técnica. La importancia de la institución dentro del internet no puede ser ignorada y por ello resultaría conveniente que nuestro país contara con un mayor acercamiento a dicha comunidad técnica y a los estándares desarrollados por esta.

### *Estándares ISO de la serie 27000*

La serie ISO/EIC 27000 corresponde a un conjunto de estándares desarrollados por la Organización Internacional para la Estandarización (ISO por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC por sus siglas en inglés), enfocados fundamentalmente al área de la gestión de la seguridad de la información. Estas normas componen un marco de referencia metódico, documentado y basado en objetivos claros, que pueden ser seguidos por toda organización (y que a su vez permiten a esta certificar su calidad) (López Neira & Ruiz Spohr, 2005).

En términos generales la serie 27000 contempla un conjunto de recomendaciones sobre mejores prácticas de manejo de la seguridad de la información, tales como los controles necesarios, los análisis de riesgo, los sistemas de privacidad del usuario, los métodos de confidencialidad, la necesidad de retroalimentación sobre el uso de la información y el manejo de impacto de los incidentes en materia de seguridad de la información.

Esta serie cubre un amplio rango de elementos publicados dentro de veintitrés estándares a la fecha (ISO 27000 Newsletter, 2006); a saber:

- ISO/IEC 27000 – Que establece los objetivos y el vocabulario básico por ser utilizado en un sistema de manejo de la seguridad de la información (SMSI).
- ISO/IEC 27001 – Que versa sobre los requisitos para los SMSI.

- ISO/IEC 27002 – Que crea un código para la práctica del manejo de la seguridad de la información.
- ISO/IEC 27003 – Que genera una guía para la implementación de SMSI.
- ISO/IEC 27004 – Que brinda un sistema de medición aplicable a los SMSI.
- ISO/IEC 27005 – Que especifica técnicas de seguridad para los SMSI.
- ISO/IEC 27006 – Que se relaciona con los requisitos para las entidades relacionadas con las auditorías y la certificación de los SMSI.
- ISO/IEC 27007 – Que establece las guías para dichas auditorías.
- ISO/IEC TR 27008 – Que provee algunas guías adicionales para el control por parte de los auditores de los controles de seguridad de las SMSI.
- ISO/IEC 27010 – Que versa sobre las comunicaciones inter-sectoriales e inter-organizacionales y las técnicas de seguridad de la información aplicables.
- ISO/IEC 27011 – Que establece guías específicas para las organizaciones de telecomunicaciones con base en ISO/IEC 27002.
- ISO/IEC 27013 – Que busca la aplicación integrada de los estándares ISO/IEC 20000-1 e ISO/IEC 27001.
- ISO/IEC 27014 – Que se relaciona con la gobernanza de la seguridad de la información.
- ISO/IEC TR 27015 – Que establece guías para ser aplicadas por los ISMI del área de servicios financieros.
- ISO/IEC 27031 – Que provee guías para las tecnologías de información y comunicación dirigidas a asegurar la continuidad de los negocios y las empresas.

- ISO/IEC 27032 – Que determina una guía sobre ciberseguridad.
- ISO/IEC 27033-1 – Que se relaciona con la seguridad de las redes, su supervisión y sus conceptos fundamentales.
- ISO/IEC 27033-2 – Que se sienta las bases del diseño y la implementación de la seguridad de las redes.
- ISO/IEC 27033-3 – Que sirve como referencia ante las amenazas, técnicas de diseño y temas relacionados con el control de las SMSI en el área de redes.
- ISO/IEC 27034 – Que establece una guía para la seguridad de las aplicaciones.
- ISO/IEC 27035 – Que versa sobre el manejo de incidentes de seguridad.
- ISO/IEC 27037 – Que procura brindar referencias relevantes al manejo, identificación, recolección y preservación de evidencias digitales.
- ISO/IEC 27799 – Que se relaciona con el manejo de la seguridad de la información en el sector salud.

Asimismo, debe mencionarse que ISO se encuentra aún trabajando en once estándares más que formarán parte de la serie 27000 y que se relacionan con los sistemas de computación en la nube, protección de datos en la nube, el área de utilidades de energía, la detección de intrusiones en SMSI, la seguridad del almacenamiento y la evidencia digital.

### *Estándar ISO 29100*

Creado en 2011 y relacionado íntimamente con la privacidad y la protección de datos personales, el estándar ISO 29100 se dedica a la creación de un marco técnico para ser utilizado por entes públicos y privados por igual, para guiar y certificar sus sistemas de protección de información personalmente identificable (IT Governance Ltd, 2011).

En términos generales, este estándar se preocupa por la creación de terminología común en materia de privacidad y la identificación de sus actores, la descripción de las principales consideraciones para ser tomadas en la protección de los datos y hace referencia a los principios más conocidos en materia de privacidad del usuario, protección de datos personales y tecnologías de la información y la comunicación.

A la vez, este estándar se detiene a explorar de manera cautelosa cuáles informaciones y datos habrán de ser protegidos por el marco por él creado; para ello explora las características fundamentales de los datos personalmente identificables, estableciendo una serie de identificadores y características distintivas, para a continuación tornar su atención en los metadatos, la información personalmente identificable "no solicitada"[214] y los datos sensibles.

Finalmente debe mencionarse que este estándar incorpora muchos de los principios ya estudiados reiteradas veces. Específicamente hace referencia al consentimiento y elección; legitimidad y especificación del propósito; limitación de la recolección; minimización de los datos; limitación del uso, retención y publicación; precisión y calidad de los datos; apertura, transparencia y notificación; participación individual y

[214] Datos personales recibidos sin que la agencia o el ente hayan tomado los pasos necesarios para recolectar dicha información, ver (Comisión de Reforma a la Ley Australiana, 2013).

acceso; responsabilidad; seguridad de la información; y cumplimiento de la privacidad (ISO/IEC, 2011).

### *Estándar ISO 22307*

Dirigido fundamentalmente al sector financiero, el estándar ISO 22307 procura la implementación de "valoraciones de privacidad"[215] a la hora de brindar servicios bancarios con miras a identificar los riesgos que el procesamiento automatizado de datos puede acarrear en los sistemas de información actuales.

Creado en 2008 y revisado en 2012 por su gran importancia, el estándar se dedica básicamente a la descripción de las actividades necesarias para valorar la protección ofrecida a los datos de los individuos, así como a servir de guía para educar al lector sobre esta materia.

En términos generales entonces, puede asegurarse que el estándar busca establecer métodos de planeamiento informado que permitan a las instituciones financieras ampliar su oferta de servicios (y revisar sus servicios actuales) en el marco de las posibilidades ofrecidas por las tecnologías de la información y la comunicación, con la seguridad de encontrarse cumpliendo con los requisitos que les impone la ley.

[215] Que se diferencia de una auditoría en tanto la valoración determina el cumplimiento actual de los requisitos legales existentes para los sistemas implementados, así como los pasos a tomar para prevenir caer en incumplimiento (International Standards Organization, 2008).

## Protocolos

Otro ejemplo de las herramientas que la industria y la academia han intentado impulsar en la búsqueda de una solución a las dificultades que enfrenta la protección de datos personales en el mundo moderno, puede ser encontrado en los protocolos[216] de telecomunicaciones.

En el ámbito de las tecnologías de la información, se llama protocolo a un conjunto especial de reglas (establecidas como parte de un estándar abierto internacional o de manera privada como estándares creados por las diversas industrias o empresas) que son utilizadas por los puntos de una red en sus comunicaciones.

Compuestas fundamentalmente por disposiciones relevantes al cifrado de los datos (criptografía), la estructura y secuencia lógica de los datos transmitidos, y los parámetros técnicos de identificación y autenticación de las partes de la comunicación, estas reglas procuran generalmente garantizar la confidencialidad, integridad, autenticación y el no repudio de la información transmitida.

Vigentes en los más diversos niveles funcionales de una red de telecomunicaciones, los protocolos permiten tanto la comunicación de los dispositivos físicos como de aplicaciones de software, gracias a que ponen en común las reglas que rigen el contenido de la comunicación, por lo que resulta natural que puedan contribuir en el futuro a los sistemas internacionales de protección de datos personales.

[216] Palabra proveniente del griego “protocollon”, la cual hacía alusión a una hoja de papel que indicaba los contenidos de un manuscrito determinado.

*Protocolo P3P*

Desarrollado por el Consorcio de la World Wide Web (W3C) y recomendado desde el 26 de abril de 2002, el protocolo de Plataforma de Preferencias de Privacidad (o P3P) establece un conjunto de reglas mediante las cuales los sitios web pueden declarar públicamente y mediante un formato estándar, sus intenciones de uso de la información que recopilan sobre sus usuarios.

El protocolo P3P propone un sistema mediante el cual tanto las páginas web como el usuario declaran los tipos de información que buscan recopilar, mientras que los usuarios determinarán qué tipo de información están dispuestos a compartir. A partir de estos datos el protocolo será capaz de informar al usuario en caso de que la página solicite más información de la que el usuario ha autorizado compartir y proporcionarle de esta manera la capacidad de tomar decisiones informadas con base en su derecho de autodeterminación informativa.

En términos generales, P3P se preocupaba por facilitar al usuario la capacidad de conocer y decidir sobre los datos personales almacenados por el servidor, su uso, permanencia y visibilidad. Ello le permitía trabajar de manera simplificada y organizada y ser compatible con gran cantidad de dispositivos y exploradores de internet.

A pesar de estas ventajas, el protocolo P3P tuvo una acogida fría por la industria y contó con muchos detractores, quienes afirmaban que la manera en que se presentaba la toma de decisiones al usuario era muy difícil y el hecho de incorporar

dichos protocolos sin contar con una base de usuarios suficientemente informados culminaría con un falso sentimiento de seguridad.

Tal como se verá más adelante, otro de los problemas que presenta esta solución es su falta de aplicabilidad real. Sin un marco legal apropiado, las decisiones del usuario frente a las políticas declaradas de la compañía no poseían ninguna ramificación legal, y nada impedía que las compañías realizaran declaraciones falsas sobre los tipos de información recopilada. Todas estas situaciones[217] llevaron finalmente a que el protocolo cayera en desuso, y si bien actualmente continúa estando disponible al público[218], cuenta con una implementación real prácticamente nula en la actualidad.

### *Protocolo Do Not Track*

Propuesto originalmente en 2009, el protocolo Do Not Track basa su sistema de protección en la incorporación de un encabezamiento a las comunicaciones informáticas, el cual solicita que toda aplicación web que lo reciba desactive sus sistemas de rastreo de usuarios. Al igual que en el caso de P3P, a la fecha el protocolo Do Not Track no puede ser aun considerado como una solución viable a los problemas de la Protección de Datos Personales, en tanto no cuenta con un apoyo substancial por parte de la industria, a la vez que tampoco cuenta con un marco legal internacional que haga vinculantes sus solicitudes.

[217] Incluyendo el hecho de que P3P no lograra realmente cumplir con las políticas justas de la información (en tanto limita su accionar a notificar al interesado y no pretende prevenir de manera real el daño potencial).
[218] Y es incluso incluido en programas como el Internet Explorer de Microsoft.

A pesar de lo anterior, el protocolo poco a poco se abre camino en la actualidad dentro de la industria de internet y cuenta con la particularidad de que ha sido incluido en navegadores de gran popularidad (Firefox, Explorer y Chrome) incluso como una opción activada por defecto (Lynch, 2012). Estas novedades han causado gran discusión y polémica, y podrían parecer, para quien decida mantenerse optimista, una nueva esperanza para la adopción y respeto de este tipo de soluciones por parte de la industria y el sector público internacional.

## Privacidad por Diseño

Este método técnico de protección de datos fue desarrollado en la década de los años 90 por la Comisionada de Información y Privacidad de Ontario, Canadá Ann Cavoukian *"para atender los efectos siempre crecientes y sistemáticos de las Tecnologías de la Información y las Comunicaciones, y de los sistemas de datos en red a gran escala"* (Cavoukian, 2001, pág. 1).

Basado en siete principios fundamentales, el método de protección por medio de la Privacidad por Diseño (PbD) procura brindar un enfoque holístico a la protección de los datos personales por medio de la implementación predeterminada de la privacidad a lo largo de todas las etapas de desarrollo e implementación de las nuevas tecnologías. Así, la privacidad por diseño *"se extiende a una "Trilogía" de aplicaciones que engloban 1)*

*sistemas de tecnologías de la información; 2) prácticas de negocio responsables; y 3) diseño físico e infraestructura en red"* (Cavoukian, 2001, pág. 1)[219].

Específicamente, los principios involucrados en las técnicas de privacidad por diseño son los siguientes:

- Proactivo, no reactivo; preventivo, no correctivo: Procura anticipar y prevenir las consecuencias relacionadas con las invasiones a la privacidad y las vulneraciones a los datos personales antes de que estas lleguen a ocurrir. Al no esperar a que los riesgos se materialicen, la PbD tampoco brinda remedios para estos[220].
- Privacidad como la configuración predeterminada: La PbD procura asegurar siempre el máximo nivel de privacidad, liberando la carga de acción tanto del individuo como del procesador de los datos, puesto que la interconstrucción de los máximos niveles de privacidad dentro del sistema asegura que esta se mantendrá intacta aún frente a la inacción individual[221].
- Privacidad incrustada en el diseño: Se procura incrustar de manera completa las medidas dirigidas a la protección de los datos personales dentro de todas y cada una de las etapas de diseño y la arquitectura misma de los sistemas informáticos y las prácticas de negocios utilizadas. No se percibe a la privacidad como un aditamento para ser agregado al sistema, sino que se considera parte esencial de las funcionalidades centrales entregadas por el sistema.

[219] Dando especial relevancia por supuesto a los datos sensibles en el proceso de protección relacionado con estas aplicaciones.
[220] Pues estos se tornan innecesarios.
[221] De esta manera, aún cuando el interesado no realice una acción (tal como solicitar que su privacidad sea respetada, como sucede en los protocolos Do Not Track), su privacidad se mantendrá intacta.

- Funcionalidad Total – "Todos ganan", no "Si alguien gana, otro pierde": Procurando asegurar situaciones de "ganar-ganar", la PbD no requiere que los interesados realicen concesiones innecesarias. *"Privacidad por Diseño evita la hipocresía de las falsas dualidades, tales como privacidad* ***versus*** *seguridad, demostrando que* ***sí es*** *posible tener ambas al mismo tiempo"* (Cavoukian, 2001, pág. 2).
- Seguridad Extremo-a-Extremo – Protección de Ciclo de Vida Completo: En tanto las disposiciones relativas a la privacidad se encuentran incrustadas dentro del proceso mismo por realizarse, la PbD se extiende a lo largo del ciclo de vida de los datos involucrados, por lo que estos son recogidos, retenidos, tratados y eliminados con seguridad, administrando seguramente la totalidad del ciclo de tratamiento de la información.
- Visibilidad y Transparencia – Mantenerlo Abierto: Mediante la implementación de procesos visibles y transparentes, la PbD *"busca asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada, esta en realidad esté operando de acuerdo con las promesas y objetivos declarados, sujeta a verificación independiente" (Cavoukian, 2001, pág. 2).*
- Respeto por la Privacidad de los Usuarios – Mantener un Enfoque Centrado en el Usuario: manteniendo al usuario como máxima prioridad de los sistemas, la PbD requiere que los arquitectos y operadores respondan fundamentalmente a los intereses de las personas, añadiendo opciones amigables con ellos, notificándoles adecuadamente y garantizando los máximos niveles predefinidos de privacidad.

### *Síntesis de la Tercera Sección*

Sistemas Internacionales

*A lo largo de la cual serán estudiados algunos de los sistemas que han propuesto soluciones legales a la problemática actual de la protección de datos personales en el ámbito internacional.*

El estudio realizado a lo largo de las dos primeras secciones de este capítulo evidencia que el tema ha sido tratado de maneras muy diversas por los diversos sistemas existentes en el nivel mundial. Estos sistemas se han caracterizado por contar con grandes variaciones en la protección por ellos reconocida a los datos personales, y como resultado, en los últimos años han surgido algunas iniciativas dirigidas a la creación de sistemas unificados (o cuando menos interoperables) que permitan superar las dificultades de la protección de datos personales en el nivel internacional; dentro de ellos encontramos los siguientes:

- Convenio 108 del Consejo de Europa:
    - Ya estudiado en la primera sección del presente capítulo, se caracteriza por ser el único instrumento legal internacional vigente en materia de protección de datos personales, que posee un ámbito de aplicación mundial y se encuentra abierto a ser firmado y ratificado por cualquier país del mundo.
- Programa de Safe Harbor:
    - Tal como se estudió anteriormente, la entrada en vigencia de la Directiva Europea 95/46/EC, implicó la prohibición de la transferencia de datos personales a aquellos países que no contaran con un nivel adecuado de protección.
    - Como se pudo observar a partir del análisis de la legislación estadounidense, este sistema se basa fundamentalmente en un sistema de auto regulación para el sector privado y de regulación mínima para el sector público (con extensas excepciones aplicables en nombre de la

seguridad nacional). Esta situación contraviene directamente las disposiciones de la Directiva europea.

- Con miras a no afectar las relaciones comerciales entre estas dos potencias, el programa de Safe Harbor se constituye como un sistema de cooperación que permite a las empresas y organizaciones interesadas en exportar e importar datos personales de la Unión Europea, autocertificar que cumplen con las disposiciones de la Directiva 95/46/EC.
- Esta autocertificación se basa en seis requisitos para las empresas, aunados con la necesaria adopción de siete principios fundamentales (notificación, elección, principios de las transferencias de datos, seguridad, integridad de los datos, y acceso).

- Protección Adecuada según Estándares Europeos:
  - Programa de certificación considerado actualmente la principal manera de determinar el nivel de protección brindado por un país a los datos personales; procura determinar si el Estado cuenta con un grado de protección superior, igual, similar o equivalente al sostenido en la Unión Europea, con miras a *"evitar la creación de paraísos informáticos (data havens), es decir, jurisdicciones donde la carencia de leyes de protección de datos, las trasforme en sitios atractivos para realizar tratamientos de datos personales que puedan ser violatorios de otras leyes de privacidad" (Remolina-Angarita, 2010, pág. 467).*
  - El análisis que lleva a esta certificación se basa en factores de naturaleza regulatoria, instrumental e institucional, que incluyen tanto el contenido del marco legal y constitucional aplicable como la realidad de la aplicación de dicha normativa en el país.
- Guías de la Organización para la Cooperación y el Desarrollo Económico:
  - Primer ejemplo de principios aceptados internacionalmente en materia de protección de datos personales; contempla disposiciones aceptadas y replicadas en el mundo entero.

  - Sus prácticas justas de la información procuran el potenciamiento de una cultura de seguridad compartida internacionalmente y se limita a la definición del tema, el establecimiento de los principios básicos y la delimitación de algunos fundamentos.
  - En tanto para finales de la década de 2000 se hizo evidente la necesidad de actualizar este instrumento, un grupo de múltiples interesados fue creado por la OCDE y en su versión de 2013 ve actualizado su enfoque práctico al adoptar una visión coordinada de las estrategias nacionales de protección de datos que contemplen el manejo de riesgos y la interoperabilidad de estos.

- Red Iberoamericana de Protección de Datos:
  - Patrocinada por la Agencia Española de Protección de Datos, la Red Iberoamericana de Protección de Datos reúne a 22 países de la región Iberoamericana (incluyendo a Costa Rica) en un foro multilateral dirigido a la armonización de la legislación nacional sobre la materia, con base en las disposiciones de la directiva Europea 95/46/CE. Ha generado un buen número de *Declaraciones* a lo largo de sus 12 años de funcionamiento que reúnen los compromisos adoptados por sus miembros.
- Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico:
  - Aprobado como parte de las metas de cooperación de los países de APEC, el marco establece un conjunto de principios fundamentales en materia de privacidad y protección de datos, a la vez que establece algunas guías para la implementación de estos en los niveles nacional y el internacional.
  - Caracterizado por su flexibilidad y por reconocer la necesaria transmisión transfronteriza de datos, el marco procura *"favorecer sistemas de protección que prevengan la restricción innecesaria del flujo de datos, balanceando la necesidad de protección con los intereses comerciales y las necesidades corporativas y el necesario reconocimiento a las diversidades de los países miembros" (Foro de Cooperación Económica Asia-Pacífico, 2005, pág. 3).*

- Establece nueve principios fundamentales, a saber: prevención del daño, notificación, limitaciones a la recolección de datos, usos de la información personal, elección, integridad, salvaguardas de la información, acceso y corrección, y responsabilidad.

- Resoluciones y Declaraciones de las Conferencias Internacionales de Autoridades de Protección de Datos y Privacidad:
  - Consideradas como los mayores foros dedicado a la regulación armoniosa de la protección de datos en el ámbito mundial, las conferencias reúnen a las más altas autoridades e instituciones relacionadas con el tema, las cuales generan resoluciones y declaraciones dirigidas a guiar a los países en la solución de problemas apremiantes. Algunas de las resoluciones más representativas han tratado los siguientes temas:
    - Appificación de la sociedad (relacionada con el rol de las aplicaciones en los nuevos dispositivos).
    - Futuro de la privacidad (en la cual se intensifica la cooperación transfronteriza de las autoridades).
    - Computación en la nube (que procura evitar la reducción de los estándares de protección de datos en los sistemas basados en la nube).
    - Creación de perfiles (recomienda asegurar la transparencia de las operaciones de *big data*).
    - Privacidad por diseño (reconoce la necesidad de implementar los principios y la supervisión de la protección de datos personales a lo largo del proceso de creación y funcionamiento de las nuevas tecnologías).
    - Estándares internacionales (que realiza una propuesta conjunta de principios internacionales).
    - Privacidad y redes sociales (enfrenta la realidad de la autogeneración de perfiles por los usuarios y plantea una serie de recomendaciones).

- Proyecto de norma ISO para la privacidad (reconoce la necesidad de proteger técnicamente los datos personales por lo que recomienda la creación de un estándar ISO que facilite tal fin).

Soluciones Técnicas Internacionales

*A lo largo de la cual serán estudiados algunas de las soluciones planteadas a la problemática internacional de la protección de datos personales desde el punto de vista técnico.*

En tanto se trata de un panorama iusinformático, el estudio de las soluciones técnicas para la protección de datos personales no puede ser olvidado; algunas de las más relevantes en la actualidad son las siguientes:

- Estándares Internacionales:
  - Estándar: "*Documento que provee requisitos, especificaciones, guías o características que pueden ser utilizados consistentemente para asegurar que materiales, productos, procesos y servicios sean adecuados para sus propósitos (…) los estándares internacionales aseguran que los productos y servicios sean seguros, confiables y de buena calidad" (International Standards Organization, 2013).*
  - RFCs de la Internet Engineering Task Force:
    - La IETF es uno de los entes internacionales más relevantes en la administración técnica del Internet, cumple un importante rol en la generación de estándares abiertos por medio de documentos conocidos como "Requests for Comments".
    - A la fecha la IETF cuenta con al menos seis RFCs relacionados directamente con la privacidad.
  - Estándares ISO:
    - Desarrollados por la Organización Internacional para la Estandarización; es posible identificar una buena cantidad de estándares que se relacionan con la protección de datos

personales en tanto procuran asegurar la protección de la información.

- Encontramos algunos ejemplos especialmente relevantes en la serie de estándares 27000 (que comprende al menos 23 estándares de seguridad de la información), el estándar 29100, y el estándar 22307.

- Protocolos:
  - Conjuntos especiales de reglas (establecidas como parte de un estándar abierto internacional o de manera privada como estándares creados por las diversas industrias o empresas) que son utilizadas por los puntos de una red a en sus diversos niveles de comunicaciones. Fundamentalmente se pueden mencionar dos protocolos relevantes en la actualidad:
    - Protocolos P3P: Establecen un conjunto de reglas mediante las cuales los sitios web pueden declarar públicamente y mediante un formato estándar sus intenciones de uso de la información que recopilan sobre sus usuarios.
    - Protocolo Do Not Track: Basan su protección en la incorporación de un encabezamiento a las comunicaciones informáticas dirigido a solicitar que toda aplicación web que lo reciba desactive sus sistemas de rastreo de usuarios.
  - Se puede afirmar que las soluciones tecnológicas basadas en protocolos enfrentan actualmente problemas, en tanto no cuentan con apoyo substancial por parte de la industria ni han sido reconocidos como vinculantes por un marco legal internacional que posibilite su aplicación.
- Privacidad por Diseño: Procura brindar un enfoque holístico a la protección de los datos personales por medio de la implementación predeterminada de la privacidad a lo largo de todas las etapas de

desarrollo e implementación de las nuevas tecnologías. Así, la privacidad por diseño *"se extiende a una "Trilogía" de aplicaciones que engloban 1) sistemas de tecnologías de la información; 2) prácticas de negocio responsables; y 3) diseño físico e infraestructura en red."* (Cavoukian, 2001, pág. 1). Sus siete principios fundamentales son:

- Proactivo y preventivo
- Privacidad predeterminada
- Privacidad incrustada
- Funcionalidad total
- Protección de ciclo de vida completo
- Visibilidad y Transparencia
- Enfoque centrado en el usuario

# Título Tercero: La protección de datos en Costa Rica: un proyecto incompleto

## Capítulo I: Marco administrativo y regulatorio de las Telecomunicaciones y la Protección de Datos Personales en Costa Rica

A lo largo del presente capítulo se habrá de realizar un estudio detallado de la situación actual de las telecomunicaciones y la protección de datos personales en Costa Rica. Se iniciará con una introducción histórica dirigida a aclarar el contexto que rodea a la situación actual de las telecomunicaciones en nuestra nación y, a continuación, se expondrá una síntesis del marco administrativo que rodea al sector telecomunicaciones.

Más adelante, se examinarán los elementos fundamentales que conforman el marco regulatorio de las telecomunicaciones, para finalmente profundizar en el estudio de la normativa que rodea a la protección de datos personales frente al panorama planteado por las telecomunicaciones convergentes en nuestro país.

## Sección I: El Estado Actual de las Telecomunicaciones en Costa Rica

### *Breve Introducción Histórica de las Telecomunicaciones en Costa Rica*

La República de Costa Rica[222] se encuentra ubicada en Centro América, su territorio está comprendido entre el Mar Caribe, el Océano Pacífico y las Repúblicas de Nicaragua y Panamá. Posee una superficie total de 51.100 $km^2$ y se encuentra dividida en siete provincias, 81 cantones y 487 distritos. Su capital se ubica en la ciudad de San José y para el 2011 contaba con una población total de 4.458.353 habitantes (Arias, 2013).

El país ha tenido una larga historia de estabilidad política y económica, y es muy conocido a lo largo del mundo por contar con un desempeño superior al promedio global en la mayoría de los indicadores sociales, especialmente en comparación con otros países del Tercer Mundo. En concreto, Costa Rica tiene actualmente un alto nivel de desarrollo humano[223] gracias principalmente al alto nivel de acceso a sus sistemas de salud pública[224] y educación[225].

Con un producto interno bruto estimado en $58.55 billones (Agencia Central de Inteligencia, 2014), el país ha tenido una larga historia de logros en variados índices de competitividad (Superintendencia de Telecomunicaciones, 2010) que en años pasados

[222] Para una visión rápida del perfil de telecomunicaciones de este país de acuerdo a la Unión Internacional de Telecomunicaciones, consulte (Unión Internacional de las Telecomunicaciones, 2012)
[223] El desarrollo humano en el país es considerado alto, al punto que se ubica en la posición Nº 62 según el último Informe de Desarrollo Humano del PNUD (United Nations Development Programme, 2013).
[224] El gobierno de Costa Rica reporta actualmente gastos de 10,9% del PIB en salud pública, lo que lo sitúa en el puesto 16 a nivel mundial, y ha llevado al país a tener una de las esperanzas de vida más altas del mundo (78,06 años) (Agencia Central de Inteligencia, 2014).
[225] Que no solo constituye el 6,3% de los gastos anuales del país (ubicándolo en la 32ª posición mundial), sino que también ha permitido al país alcanzar un grado de alfabetización total superior al 96,3%. (Agencia Central de Inteligencia, 2014).

han permitido el crecimiento sostenido del mercado de las tecnologías de información y comunicación en el país[226].

Las razones para la larga historia de estabilidad que caracteriza a Costa Rica pueden ser atribuidas al marco político y jurídico establecido por la Constitución Política de Costa Rica de 1949[227], la cual fortaleció el sistema democrático, abolió el ejército, defendió los derechos humanos y constituyó el punto de partida de un ambicioso proyecto político de reforma jurídica y económica[228] que dio forma al país durante las siguientes tres décadas[229].

Una de las consecuencias más importantes de este nuevo marco legal fue la fundación del "Instituto Costarricense de Electricidad" (ICE), una institución autónoma, con completa independencia administrativa, cuya misión fundamental era el desarrollo, implementación y comercialización de energía eléctrica en todo el país y de los servicios de telecomunicaciones mediante un régimen de monopolio estatal.

[226] La penetración del internet en el país ha aumentado continuamente en los últimos años, y de acuerdo con estimaciones del Banco Mundial, en 2013 el 45% de la población de Costa Rica tenía acceso a Internet (Banco Mundial, 2013). Este y otros elementos han sido fundamentales para permitir la expansión del Sector Telecomunicaciones de Costa Rica a su punto actual, donde su mercado constituye el 3,3% del PIB del país (Cordero Sancho, 2013).

[227] Que puede ser caracterizada como la principal consecuencia de la guerra civil de 1948, uno de los pocos ejemplos de conflictos militares en la historia costarricense que culminó con la victoria de la fracción de José Figueres Ferrer, la cual logró derrocar al presidente Rafael Ángel Calderón Guardia del poder para a continuación instaurar un gobierno temporal.
Durante el año de duración de dicho gobierno, Figueres realizó importantes reformas en nuestro país: abolió el ejército, introdujo el derecho de las mujeres al voto, aseguró la educación pública y dicto alrededor de 834 políticas dirigidas a asegurar el bienestar del pueblo. Asimismo, durante dicho año fue formada una Asamblea Constituyente que redactó la nueva Constitución Política del país (Veillette, 2005).

[228] Estas reformas se basan en la doctrina de Estado de Bienestar. Este sistema fue sustituido a finales de los 80, cuando la globalización llevó a nuestra economía hacia un sistema cada vez más neoliberal.

[229] Para obtener más información acerca de la historia de Costa Rica, las razones de sus muchas diferencias con respecto a sus vecinos de América Central y su relación con el Gobierno de EE.UU., Ver (Veillette, 2005), y para un estudio específico sobre las dificultades de la liberalización del mercado de las telecomunicaciones en el país es muy recomendable que el lector revise el trabajo de (Hoffman, 2008).

En el momento de su creación, las responsabilidades del Instituto se limitaron al desarrollo del sistema eléctrico del país. Sin embargo, en 1963 la Asamblea Legislativa de Costa Rica aprobó la Ley N º 2336 que otorgó al ICE y a sus empresas filiales, el deber de establecer, mejorar, ampliar y operar los servicios de telefonía, telegrafía y radiotelefonía del país.

Entre estas nuevas responsabilidades, el ICE tenía la obligación de representar al país ante varias organizaciones internacionales (como la UIT), y asumir la dirección de las actividades de desarrollo relacionadas con la infraestructura nacional de telecomunicaciones. Estos factores a su vez implicaron que durante la mayor parte de su historia, el ICE tuviera completa autoridad sobre las decisiones técnicas y la adopción de estándares de telecomunicaciones específicos en el país.

El ICE se destacó en el cumplimiento de sus deberes, y para finales de la década de 1970 había conectado a todo el país mediante una red pública de telecomunicaciones y totalmente automatizada; la cual no solo proporcionaba tasas subsidiadas a los habitantes de la República, sino que también contaba con una extensa red de teléfonos públicos en todo el país como parte de sus múltiples programas dirigidos al fomento del bienestar social.

En palabras de Hoffman: *"En contraste con el enfoque que prevalece en la mayor parte del Tercer Mundo, el modelo costarricense vio a las telecomunicaciones no como un artículo de lujo para las élites urbanas, sino como una función esencial de la integración y el desarrollo nacional. Como resultado, Costa Rica goza de una de las redes de telefonía más densas y socialmente equilibrada de todos los países en desarrollo "* (Hoffman, 2008).

La importancia de este contraste no puede ser subestimada, ya que demuestra la magnitud de la función del ICE dentro de las reformas políticas "socialdemócratas" llevadas a cabo en el país, mediante las cuales el Instituto se convirtió en uno de los pilares fundamentales del progreso y el bienestar nacional. En este contexto, el papel del ICE se tornó fundamental durante los años 1970 y 1980, pues fue en esta época cuando la institución realizó algunas de sus más grandes inversiones en infraestructura eléctrica y de telecomunicaciones[230]. Dichas inversiones afectaron positivamente a todos los sectores de la sociedad costarricense y llevaron a la incorporación, dentro de la opinión pública, de un sentimiento generalizado de aprecio y respeto por la institución[231].

La década de 1990 conllevó para nuestra nación la implementación generalizada de redes de telecomunicaciones digitales. Durante 1991, la Universidad de Costa Rica (UCR)[232] y Radiográfica Costarricense SA (RACSA)[233] instalaron con éxito las primeras redes de datos del país[234] (De Theramond, 1994). El éxito de este proyecto conjunto se

[230] La institución realizó un gran esfuerzo en sus luchas por dotar a nuestro país con infraestructura de primera calidad. Este propósito se vio directamente traducido en algunos de los mayores avances en materia de extensión de la infraestructura eléctrica y telefónica nacional, tales como la construcción del embalse Arenal (la segunda mayor reserva de agua artificial de Centroamérica) y la implementación a gran escala de redes de microondas y por satélite que conectaron el país con la red telefónica internacional.

[231] Este sentimiento se ha mantenido hasta nuestros días, y a pesar de su condición actual, el ICE todavía es considerado por muchos costarricenses como "La institución por excelencia para el orgullo nacional de Costa Rica" (Hoffman, 2008).

[232] La Universidad de Costa Rica es una de las cuatro universidades públicas del país y fue una institución pionera en los proyectos por crear las primeras redes de datos del país. Está claro sin embargo, que la UCR no fue la única institución académica a participar, ya que con el tiempo todas las universidades públicas del país han contribuido al éxito de los proyectos posteriores, como el desarrollo de la primera red de datos académica del país, la “Red Nacional de Investigación” (De Theramond, 1994).

[233] Una de las compañías subsidiarias del ICE dedicados al desarrollo de las telecomunicaciones en Costa Rica, que compartían con el ICE la concesión exclusiva para la explotación de servicios de telecomunicaciones antes de la liberalización del sector.

[234] Cuyos primeros pasos fueron la conexión de las computadoras de la UCR a la Bitnet y posteriormente al Internet. Asimismo, proyectos subsecuentes lograron crear una red troncal de datos para todo el país

constituyó como un punto fundamental para la oferta comercial de accesos a internet que comenzara a darse en 1994[235] y para otros grandes desarrollos realizados durante la década, tales como la obtención de la primera conexión internacional de fibra óptica mediante el anclaje del cable submarino MAYA-1 en nuestro país.

Esta década también se caracterizó por acercar la economía de nuestro país a su inmersión completa en los mercados liberalizados globales. En 1994 el presidente José María Figueres Olsen propuso la venta del ICE y la privatización de la electricidad y el monopolio de las telecomunicaciones; un paso que requerido como parte de la agenda de liberalización perseguida por el gobierno desde la década de 1980[236]. Esta propuesta fue recibida con protestas inmediatas, por lo que el gobierno se vio obligado a dejar de lado su táctica inicial y a dirigirse hacia un nuevo camino: *"En lugar de perseguir la privatización a través de la venta de la ICE, (el gobierno) buscó dejar la compañía en su sitio, pero romper su monopolio invitando a la competencia privada "(Hoffman, 2008).*

Este proyecto no podría ejecutarse sino hasta después de las elecciones de 1998, cuando fuera adoptado por el recién electo presidente Miguel Ángel Rodríguez. Con miras a lograr este objetivo, Rodríguez presentó tres proyectos de ley a la Asamblea

sobre la base de la infraestructura óptica (instalada por el ICE y RACSA) que ya conectaba a nuestras principales ciudades (De Theramond, 1994).

[235] Originalmente ofrecida al público únicamente por RACSA mediante un convenio con la Academia Nacional de Ciencias (ANC), la cual es una institución pública, no gubernamental, reconocida oficialmente por la Ley N º 7544 de 1995. Esta organización se encuentra encargada de la administración del dominio de nivel superior geográfico ".cr" desde 1990 a través de su ente dependiente "NIC - Internet Costa Rica".

[236] Como se indicó anteriormente, en 1980, la crisis de la deuda externa debilitó la economía de Costa Rica y puso fin a la mayor parte de las políticas del Estado de Bienestar que habían sido adoptadas por el Gobierno desde 1949. En este contexto, el gobierno firmó un acuerdo de estabilización con el Fondo Monetario Internacional, que requirió que el país comenzara a implementar una serie de programas de ajuste estructural que "englobaron la reducción de los gastos del Estado para reducir el déficit presupuestario, la reducción de los subsidios, la adopción de un estrategia de crecimiento impulsado por las exportaciones, y la privatización de las empresas estatales " (Hoffman, 2008).

Legislativa de Costa Rica: una ley orgánica general para el ICE[237], una nueva ley para el sector de la energía y un proyecto de ley de telecomunicaciones. Este segundo paso hacia la privatización también generó múltiples manifestaciones de rechazo que evidenciaban un descontento popular generalizado. A pesar de ello, el gobierno insistió en sus esfuerzos hasta el punto de que la situación degeneró en una serie de huelgas dentro del sector público, dirigidas a defender el papel del ICE como institución pública. Conocidas como las protestas del "Combo", este movimiento popular logró paralizar el país durante dos semanas hasta que el Gobierno se vio forzado, una vez más, a dar marcha atrás.

Con base en dicha situación, la administración del presidente Rodríguez buscó implementar algunas políticas tendientes a apoyar el tránsito de la "economía costarricense posmoderna" hacia una economía digital. Para ello en 2001 el presidente Rodríguez dio a conocer una "agenda digital" como parte de su "Programa Impulso". Esta agenda procuraba ser implementada sin requerir la aprobación de nuevas leyes y vino a caracterizarse como el primer esfuerzo gubernamental para desarrollar un marco de política general para la adopción de las tecnologías de información y comunicación en Costa Rica[238].

A pesar de lo anterior, en el 2002, la cuestión de la liberalización de las telecomunicaciones fue nuevamente puesta en el tapete político de Costa Rica como parte de las negociaciones del Tratado de Libre Comercio de Centroamérica (CAFTA), el

[237] Que pretendía separar los sectores de electricidad y telecomunicaciones de la compañía.
[238] Para lo cual este programa procuró introducir temas como el gobierno electrónico, la protección de datos personales y la brecha digital a la agenda política de nuestro país. De esta manera este programa establece un hito en el desarrollo de políticas en materia de tecnologías de la información en nuestro país y se convirtió en un precursor directo de los actuales Planes Nacionales de Desarrollo de las Telecomunicaciones.

cual dirigió al Gobierno de Costa Rica hacia la reformulación de sus estrategias pasadas. *"Si bien el proyecto inicial incluía disposiciones para abrir totalmente el sector de las telecomunicaciones a la competencia privada, el gobierno de Costa Rica renegoció esta parte. Concedió la apertura de los servicios de Internet, telefonía móvil y servicios de redes de datos, pero no el monopolio del ICE en telefonía de línea principal y la electricidad. El 25 de enero de 2004, el gobierno de Costa Rica finalizó las negociaciones con los EE.UU. y se unió al CAFTA – quedando tan solo pendientes su ratificación por el Congreso de EE.UU. y la Asamblea Legislativa de Costa Rica"* (Hoffman, 2008).

Mientras que la ratificación del DR-CAFTA[239] por el Congreso de EE.UU. fue llevada a cabo en el 2005, una serie de acontecimientos atrasaron la ratificación del tratado por parte de Costa Rica hasta 2007, cuando la amplia oposición popular a la ratificación del tratado obligó al presidente Oscar Arias a convocar a un referéndum sobre el tema. Este referéndum fue finalmente celebrado el 7 de octubre de 2007 y culminó con la aprobación del tratado por un margen muy estrecho (51,6 sobre 48,4 por ciento) a pesar de ser evidenciada una larga lista de irregularidades antes y durante la realización de este.

La ratificación del DR-CAFTA por la Asamblea Legislativa el 21 de noviembre de 2007, conllevó también una larga lista de reformas legales complementarias (mejor conocida como la "agenda de implementación ") que nuestro país debió adoptar a fin de cumplir con sus nuevos deberes respecto a sus socios comerciales. Entre estas reformas, el país se vio obligado a elaborar, en un plazo muy corto, un nuevo marco legislativo y

[239] Nombre dado al CAFTA después de la incorporación de República Dominicana al acuerdo.

administrativo que garantizara la equidad y la apertura del mercado de telecomunicaciones recientemente liberalizado.

Con el fin de cumplir con estas obligaciones, la Asamblea Legislativa de Costa Rica aprobó rápidamente el proyecto de ley correspondiente a la Ley General de Telecomunicaciones N º 8642, y posteriormente aplicó un procedimiento resumido para el estudio del proyecto de ley "sobre el fortalecimiento y modernización de las entidades públicas en el sector de las telecomunicaciones", que una vez aprobado se tornó en la Ley N º 8660 del 29 de julio de 2008.

La aprobación de la Ley N º 8660 resultó ser de suma importancia para las reformas administrativas requeridas como parte de la agenda de implementación del DR-CAFTA. No solo formalizó el fin del monopolio del ICE en telecomunicaciones nacionales, sino que también creó oficialmente el *sector telecomunicaciones* en Costa Rica, a la vez que estableció concretamente las funciones y responsabilidades de los actores que participan actualmente en dicho sector.

### *Entes Nacionales Encargados de la Regulación de las Telecomunicaciones y de la Protección de Datos Personales*

En la actualidad, el sector de las telecomunicaciones de Costa Rica se encuentra conformado por los siguientes actores:

## Poder Ejecutivo

De acuerdo con las disposiciones de la Ley N º 8660, el primer y principal agente del sector de las telecomunicaciones en el país es la administración pública. Representada por el Presidente de la República de Costa Rica y los ministros relacionados (directa o indirectamente) con el sector de telecomunicaciones, el papel fundamental que desempeña el Poder Ejecutivo en el proceso de desarrollo político del país es innegable.

### *Presidente de la República de Costa Rica*

*Sitio web: www.presidencia.go.cr*

La principal responsabilidad del Presidente de la República de Costa Rica, de acuerdo con el derecho administrativo costarricense y el marco específico del sector de las telecomunicaciones, es ejercer un papel de dirección en el proceso de desarrollo político del país[240]. Así, le corresponde a dicho funcionario el desarrollo de las

[240] Esto según las disposiciones de los artículos 22, 99 y 100 de la Ley General de la Administración Pública N º 6227, que no sólo establecen la composición del Consejo de Ministros del Gobierno, así como la relación que existe entre el presidente y sus ministros, sino que también establece un régimen político que fortalece las capacidades directivas del gobierno.
Específicamente, la ley N º 6.227 permite al Presidente de la República el ejercer la rectoría política (entendida como la facultad y capacidad para dirigir las actividades de los diversos agentes económicos en el logro de los objetivos y metas de desarrollo nacional del Estado) del país y ejercer la rectoría (junto con un ministro especializado) en sectores determinados por la ley. A través de esta rectoría, tanto el presidente como el ministro competente (o el viceministro en su defecto) podrán ordenar, a través de decretos, directivas y otros instrumentos jurídicos, las diversas actividades de cada sector y sus instituciones pertinentes.
De acuerdo con la Ley General de la Administración Pública, el papel del Presidente en el proceso de formulación de políticas es el de un "dirigente", capaz de ordenar un conjunto específico de objetivos y medios para sus ministros, pero no de determinar las actividades específicas a ser adoptadas por cualquier ministro o ministerio (que, por tanto, se encontrara habilitado para ejercer a discreción las actividades necesarias para cumplir los objetivos de acuerdo a las circunstancias del momento).

directrices generales que dirigirán las actividades de sus ministros y, hasta cierto punto, aquellas actividades de las empresas de propiedad del Estado que intervienen en el sector de las telecomunicaciones[241].

En concreto, el Presidente tiene la obligación de detallar los objetivos y los medios para el sector de las telecomunicaciones mediante el desarrollo del Plan Nacional de Desarrollo de las Telecomunicaciones (PNDT)[242] en cooperación directa con los representantes del Ministerio de Planificación Nacional y Política Económica (MIDEPLAN) y el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). El Ejecutivo en su conjunto, también debe velar por la implementación del PNDT durante el plazo del plan.

El Presidente también es responsable (junto con el Ministro de Ciencia, Tecnología y Telecomunicaciones) del desarrollo del Plan Nacional de Atribución de Frecuencias que deberá designar las diversas bandas del espectro radio-eléctrico disponibles en el país, así como su uso propuesto. Se debe señalar que de acuerdo con la Ley N º 8642, ambos funcionarios del gobierno están obligados a tomar en consideración las recomendaciones específicas emitidas al respecto por la Unión Internacional de Telecomunicaciones y de la Comisión Interamericana de Telecomunicaciones (CITEL).

[241] Al romper el monopolio del ICE sobre el mercado de las telecomunicaciones sin privatizarlo, la Ley Nº 8660 confirió un grado adicional de la independencia a ICE con el fin de permitir a la institución competir lealmente dentro del nuevo mercado de las telecomunicaciones. Esto puede ser ejemplificado por el artículo 13 de esta ley, el cual prohíbe las restricciones ilegales impuestas por el Estado sobre las inversiones del ICE, y prohíbe al gobierno a exigir la transferencia de cualquiera de los excedentes del ICE a las arcas gubernamentales.

[242] De acuerdo con la legislación nacional, el presidente de Costa Rica será también responsable de la creación de un Plan Nacional de Desarrollo (PND). El PNDT sustituirá aquellas disposiciones de carácter general sobre el sector telecomunicaciones que podrían verse incluidas en el PND, ya que poseerá un mayor grado de especificidad y especialización en sus objetivos.

Por último, de acuerdo con la Constitución de Costa Rica, es responsabilidad del Presidente y del respectivo ministro el aprobar y firmar cualquier decreto, acuerdo, resolución y o directriz ejecutiva, antes de que estos puedan ser considerados manifestaciones válidas de la voluntad del Poder Ejecutivo.

### *Ministerios*

Mediante la normativa administrativa de Costa Rica, un Ministerio es un órgano especializado del Poder Ejecutivo, el cual solo puede ser creado por ley[243]. Liderado por un ministro (nombrado personalmente por el Presidente), cada ministerio se centra en un tema determinado o tarea gubernamental y ejecuta acciones específicas para la gestión de esa área específica de gobierno. Estas acciones deben seguir y basarse en los objetivos específicos y los medios asignados para tales fines, en las directrices ejecutivas dirigidas por el Presidente de la República a cada ministro.

Actualmente el Poder Ejecutivo de Costa Rica cuenta con quince carteras ministeriales detalladas en el artículo 23 de la ley N º 6227. De ellos, los siguientes están relacionados con el sector de las telecomunicaciones y la protección de datos personales:

*Ministerio de Ciencia, Tecnología y Telecomunicaciones*

*Sitio web: www.micit.go.cr*

[243] Según el artículo 141 de la Constitución de Costa Rica y el artículo 24 de la Ley N º 6227.

Creado por la Ley N º 7169 el 26 de junio de 1990, el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) es el órgano especializado del Poder Ejecutivo encargado de definir los mecanismos y niveles de coordinación, asesoramiento y ejecución, para la consulta entre los sectores involucrados en actividades científicas y tecnológicas nacionales, y establecer su competencia y estructura organizacional (Asamblea Legislativa de la República de Costa Rica, 1990).

Las responsabilidades actuales de MICITT incluyen:

a) Definir la política de ciencia y tecnología a través de la utilización de los mecanismos de consulta establecidos por el Sistema Nacional de Ciencia y Tecnología, y contribuir con la integración de dicha política con la política general de carácter económico y social del país, en la cual actuará como enlace y contacto directo con los cuerpos de más alta decisión política del Gobierno de la República.
b) Coordinar el trabajo del Sistema Nacional de Ciencia y Tecnología por medio de la administración ejercida por el Ministro de Ciencia, Tecnología y Telecomunicaciones.
c) Desarrollar, implementar y realizar el seguimiento del Programa Nacional de Ciencia y Tecnología, de acuerdo con las disposiciones de la ley, y en el marco de coordinación del Sistema Nacional de Ciencia y Tecnología.
d) Promover la creación y el perfeccionamiento de los instrumentos legales y administrativos para el desarrollo científico y tecnológico.

e) Apoyar las funciones del Ministerio de Planificación Nacional y Política Económica en el ámbito de la cooperación técnica internacional, hacia el fomento de las actividades científicas y tecnológicas.

f) Ejercer la rectoría del sector de las telecomunicaciones mediante la generación de políticas públicas que permitan el logro de los objetivos enumerados en el artículo 2 de la Ley N º 8642 (Ley General de Telecomunicaciones).

g) Como rector del sector de telecomunicaciones, observar y cumplir con los principios rectores[244] que se enumeran en el artículo 3 de la Ley N º 8642.

En el caso concreto en estudio, es importante destacar las responsabilidades establecidas en los puntos f) y g), pues están muy relacionados con el desarrollo de políticas y la adopción de estándares técnicos en el país. El artículo 39 de la Ley Nº 8660 encomienda al Ministerio de Ciencia, Tecnología y Telecomunicaciones la rectoría del sector de telecomunicaciones de Costa Rica. Dicha tarea ha sido definida por la el PNDT como la *"dirección y coordinación de la ejecución de las políticas sectoriales públicas y estrategias desarrolladas por el poder ejecutivo"* (Poder Ejecutivo de la República de Costa Rica, 2009). Según el artículo 6 del Decreto Ejecutivo D.E. 34582-MP-PLAN, las responsabilidades específicas de cualquier ministro que ejerce la rectoría de un sector son:

a) Aprobar en forma conjunta el plan gubernamental sectorial con el Presidente de la República, de acuerdo con el Plan Nacional de Desarrollo.

[244] Estos principios son los siguientes: servicio universal, solidaridad, beneficio al usuario; transparencia; publicidad; competencia efectiva; no discriminación; neutralidad tecnológica; optimización de los recursos escasos; privacidad de la información, y la sostenibilidad ambiental.

b) Dirigir y coordinar las políticas sectoriales en las diversas instituciones del sector.

c) Dirigir y coordinar las Secretarías Sectoriales respectivas.

d) Presidir el Consejo Sectorial.

e) Asegurar que las instituciones del sector cumplen adecuadamente los objetivos (del sector), así como los lineamientos de política sectoriales existentes.

f) Autoevaluar la eficiencia y la efectividad de los resultados obtenidos por las diversas instituciones en la implementación de estrategias y políticas sectoriales.

g) Establecer mecanismos para integrar, de manera participativa, las opiniones de las distintas partes interesadas sobre asuntos de importancia y vinculación sectorial.

h) Dar su aprobación al Ministerio de Planificación Nacional y Política Económica para la incorporación de las enmiendas al Plan Nacional de Desarrollo, de acuerdo con las peticiones de cualquier jerarca institucional (Poder Ejecutivo de la República de Costa Rica, 2008).

Finalmente, se debe resaltar que en la actualidad la mayoría de estas tareas fueron delegadas por el Ministro de Ciencia, Tecnología y Telecomunicaciones en el Viceministro de Telecomunicaciones, quien preside un órgano institucional dentro del Ministerio, encargado de la ejecución de tareas específicamente relacionadas con la

rectoría de Costa Rica del sector de telecomunicaciones: el Viceministerio de Telecomunicaciones[245].

### Viceministerio de Telecomunicaciones

*Sitio web: www.telecom.go.cr*

Originalmente creado como un departamento específico del Ministerio de Ambiente y Energía y posteriormente transferido al Ministerio de Ciencia, Tecnología y Telecomunicaciones[246], el Viceministerio de Telecomunicaciones fue creado en 2008 con la aprobación de la Ley N º 8660. Esta ley define claramente tres funciones para ser adoptadas por el Estado en el recién liberalizado sector de las telecomunicaciones: rector, regulador y operador. De acuerdo con esta división, el Viceministerio de

[245] Un órgano político creado por los artículos 47 y 48 de la ley N º 6227 que establece que "El Presidente de la República podrá nombrar Viceministros (...), que sustituirán en sus ausencias temporales a los respectivos Ministros, cuando así lo disponga el Presidente de la República (y) será el superior jerárquico inmediato de todo el personal del Ministerio, sin perjuicio de las potestades del Ministro al respecto" (Asamblea Legislativa de la República de Costa Rica, 1978), cuyas principales responsabilidades incluyen la dirección y coordinación de las actividades ministeriales internas y externas, haciéndose responsable de las tareas principales de comunicación del viceministerio y la delegación, sustitución o subrogación de cualquier función dentro de los límites legales existentes, a fin de garantizar el buen desempeño del ministerio.

[246] La Ley N º 8660 originalmente encomendó la rectoría del sector de telecomunicaciones del país a un órgano especializado (la Rectoría de Telecomunicaciones) del antiguo Ministerio de Ambiente, Energía y Telecomunicaciones (MINAET).
Esta situación fue objeto de un amplio debate en su momento. Al parecer, la organización original fue realizada de esa manera con miras a reducir al mínimo los roces que podrían darse tras el cambio en el sector telecomunicaciones al dejar de encontrarse bajo el monopolio del ICE (especialmente al conservar bajo un mismo techo la potestad gubernamental de adoptar decisiones técnicas que se relacionadas con los servicios de electricidad y telecomunicaciones). A pesar de estas buenas intenciones, pronto se hizo evidente que la relación entre el sector de las telecomunicaciones y el sector de la electricidad ya no eran tan fuertes como lo eran antes de la aprobación del DR -CAFTA (sobre todo porque la generación de electricidad continuó siendo un monopolio estatal tras el tratado mientras que el mercado de las telecomunicaciones se encontraba en el medio de un fuerte proceso de liberalización).
Por otra parte, teniendo en cuenta que el país ya tenía un Ministerio dedicado a la Ciencia y la Tecnología resultaba evidente que el MINAET no era el Ministerio más adecuado para el manejo de un sector tan importante. Esta situación (junto con la presión del sector empresarial) llevó a la Asamblea Legislativa a discutir la transferencia de la Rectoría hacia el MICIT (que se convertiría en MICITT) desde el año 2009, siendo aprobada la transferencia hasta 2013 mediante la Ley N º 9046.

Telecomunicaciones se convirtió en un órgano administrativo especializado, localizado dentro de MICITT, que actualmente se encuentra a cargo de la mayoría de las tareas operativas relacionadas con el soporte de la rectoría del sector, ejercida, como se manifestó anteriormente, por el Ministro de Ciencia, Tecnología y Telecomunicaciones.

En términos generales, los objetivos fundamentales del Viceministerio son los siguientes:

a) La consolidación de la estructura organizativa que le permita al ministro cumplir con sus responsabilidades.
b) Dirigir la actividad de los diversos agentes económicos hacia el logro de los objetivos y metas del Plan Nacional de Desarrollo de las Telecomunicaciones.
c) Elaborar el Plan Nacional de Desarrollo de las Telecomunicaciones (con el apoyo de la oficina del Presidente y el Ministerio de Planificación Nacional y Política Económica) y cualquier reglamento ejecutivo aplicable al sector.
d) Desarrollar estrategias que garanticen la independencia, la transparencia, la agilidad y la eficacia de las estructuras organizativas encargadas de la regulación, administración, ejecución y control del sector.
e) Proporcionar representación internacional especializada para el país ante los organismos internacionales.
f) Aprobar o rechazar los criterios técnicos de la SUTEL en lo relativo a la adjudicación, prórroga, extinción, resolución, asignación, reasignación y rescate de las concesiones y permisos del espectro radioeléctrico.

g) La promoción de las servidumbres y expropiaciones necesarias para el avance de la infraestructura de telecomunicaciones del país y declarar el interés público de tales procesos.
h) Crear políticas específicas relacionadas con el sector y garantizar que las entidades públicas y privadas cumplan con dichas políticas.
i) Velar por el cumplimiento de la normativa ambiental y promover la gestión integral de residuos y la optimización de los recursos en todo el sector de las telecomunicaciones.
j) Coordinar las políticas de desarrollo con otras políticas públicas.

El Viceministerio de Telecomunicaciones está actualmente dirigido por el Viceministro de Telecomunicaciones y está dividido en cuatro grandes departamentos: la Dirección de Espectro Radioeléctrico, la Dirección de Redes y sistemas de Telecomunicaciones, la Dirección de Planificación y la dirección de Normas y Procedimientos.

Dentro de esta estructura administrativa, se pueden encontrar varias "gerencias" cuyas labores evidentemente se encontrarán relacionadas con las telecomunicaciones, pero que también se encuentran relacionadas con la protección de datos personales; dentro de ellas se encuentran la Gerencia de Representaciones Internacionales, la Gerencia de Sistemas de Telecomunicaciones y la Gerencia de Sociedad de la Información.

*Otros Ministerios Relacionados con el Sector Telecomunicaciones*

Ministerio de Educación Pública

*Sitio web: www.mep.go.cr*

Creado por el artículo 23, inciso j de la Ley N º 6227, el Ministerio de Educación Pública (MEP) es el órgano ejecutivo responsable de la promoción y el mantenimiento de un sistema de educación pública de alta calidad en todo el país.

De acuerdo con las disposiciones del Plan de Desarrollo Nacional de Telecomunicaciones, el Ministerio de Educación es un actor fundamental en el enfoque gubernamental para el desarrollo del sector nacional de las telecomunicaciones. En concreto, el MEP contribuye a los objetivos y tareas comprendidas dentro de la línea estratégica "Educación y capacitación" del Eje Social del Plan (MINAET - Viceministerio de Telecomunicaciones, 2012).

En particular, este Ministerio se encarga actualmente de tres acciones:

a) Proporcionar conectividad a internet de banda ancha para preescolares, escuelas y liceos del sistema público de educación (brindando una alta prioridad a aquellos centros ubicados en las zonas menos desarrolladas).
b) Proporcionar a cada centro escolar o colegial con un centro de formación de profesores equipado con infraestructura de videoconferencia educativa, multimedia y de internet.
c) Aumentar el número de estudiantes y profesores que poseen un computador personal y acceso a internet en las escuelas unidocentes.

El Ministerio de Educación ha colaborado ampliamente con la SUTEL para realizar estas tareas y en la actualidad se encuentra implementando varios programas relacionados

con la tecnología; tales como la creación de una plataforma digital para el aprendizaje del inglés, el uso de las tecnologías móviles en los contextos educativos, el fomento de proyectos de investigación relacionados con la innovación, la enseñanza a distancia a través de sistemas multimedia por internet. Asimismo, actualmente participa en un proyecto conjunto con INTEL, dirigido a renovar la infraestructura tecnológica de tres de sus centros educativos integrados.

### Ministerio de Salud

*Sitio web: www.ministeriodesalud.go.cr*

Con una historia que se remonta a 1907[247], el Ministerio de Salud es el ente rector del sector salud de Costa Rica y el órgano ejecutivo encargado de la elaboración y aplicación de políticas de salud pública preventivas.

De acuerdo con el PNDT, este ministerio es responsable de la ejecución de los objetivos y las tareas comprendidas dentro de la línea estratégica "Salud" del eje social y de la línea estratégica "Gestión de residuos electrónicos" del eje ambiental del plan (Poder Ejecutivo de la República de Costa Rica, 2009).

En concreto, el Ministerio de Salud participa en las siguientes tareas:

a) El asegurar la conectividad a internet de banda ancha a los hospitales, clínicas y demás centros de salud comunitarios de la Caja Costarricense de Seguro Social, así como a todas las sedes del Ministerio de Salud en todo el país.

[247] Para una historia más detallada de esta institución, ver (Editorial Revista Hospitales de Costa Rica, 1997)

b) El desarrollo de la red tecnológica de educación en salud a la población. Esta red utilizará estrategias tales como software especializado, portales web especializados, sistemas de teleconferencia comunitaria, otros. Se dará énfasis a poblaciones de zonas urbano-marginales, poblaciones indígenas, el binomio madre-hijo, las poblaciones con discapacidad y los adultos mayores.
c) La creación de una línea de financiamiento para proyectos dirigidos a la operación de aplicaciones de TIC en la prestación de servicios de salud (expediente electrónico, telemedicina, citas electrónicas, otros).
d) El desarrollo de las condiciones que garanticen una gestión integral de los residuos electrónicos y tecnológicos que se derivan de las tecnologías de la información y comunicación (que incluye el desarrollo de diversas normas con el apoyo del Viceministerio de Telecomunicaciones).
e) Atraer inversiones nacionales e internacionales para la valorización y eliminación de residuos electrónicos y tecnológicos.
f) Asumir todos los gastos relacionados con la ejecución de estas tareas a través de los ingresos generados por un "impuesto verde" (MINAET - Viceministerio de Telecomunicaciones, 2012).

Este ministerio también se encuentra trabajando en varios proyectos relacionados con la tecnología , tales como el desarrollo y la implantación del expediente digital único de salud, proyecto muy discutido y aprobado recientemente por la Asamblea Legislativa como Ley N º 9162, el cual contempla entre sus objetivos *"promover la interoperabilidad de la información , el procesamiento, confidencialidad, la seguridad y el uso*

*de estándares y protocolos entre las diversas entidades del sector de la salud*" (Asamblea Legislativa de la República de Costa Rica, 2013).

### Ministerio de Planificación Nacional y Política Económica

*Sitio web: www.mideplan.go.cr*

Es un ministerio importante en el desarrollo del sector nacional de telecomunicaciones, el Ministerio de Política Nacional de Planificación y Económica (MIDEPLAN) fue creado por la Ley N º 5525 del 2 de mayo de 1974, la cual lo constituye como un organismo especializado encargado de formular, coordinar, supervisar y evaluar las estrategias y prioridades del Gobierno. En otras palabras, define las visiones y objetivos para ser aplicados en el mediano y largo plazo con miras a sustentar las acciones del Poder Ejecutivo.

Entre sus principales responsabilidades, MIDEPLAN está involucrado en el desarrollo tanto del Plan de Desarrollo Nacional y el Plan Nacional de Desarrollo de las Telecomunicaciones, los cuales, como se estableció anteriormente, dirigen las actividades y decisiones del Viceministerio de Telecomunicaciones[248]. Para tal fin, la ley Nº 8660 creó el "Concejo Consultivo en Energía y Telecomunicaciones"[249], que posee la capacidad de evaluar y recomendar medidas adicionales en materia de planeamiento al Poder Ejecutivo cuando sea necesario.

[248] Esta tarea incluye la definición de responsabilidades y competencias institucionales. Esto se ha tornado en un tema importante para la administración de la presidenta Laura Chinchilla ya que varios conflictos de planificación institucional han dificultado en gran medida la aplicación de las políticas de gobierno electrónico de nuestro país.

[249] Integrado por el Presidente del Banco Central, el ministro de Hacienda, el ministro de Economía, Industria y Comercio, el Ministro de Planificación Nacional y Política Económica, y el ministro rector.

### Ministerio de Cultura, Juventud y Deportes

*Sitio web: www.mcj.go.cr*

Creado por la Ley N º 4788 el 05 julio de 1971, el Ministerio de Cultura, Juventud y Deportes (MCJD) es el organismo especializado encargado de dirigir los programas culturales y de deporte del país, incluyendo el Sistema Nacional de Bibliotecas.

La relación de este ministerio con el sector de las telecomunicaciones, se limita[250] fundamentalmente a la consecución de su papel en el eje social del Plan Nacional de Desarrollo de las Telecomunicaciones, que establece su obligación de *"proveer de acceso a Internet de banda ancha de calidad comercial a todas las bibliotecas públicas en el país, asegurando la creación de bibliotecas digitales y fomentando el patrimonio cultural del país"* (Poder Ejecutivo de la República de Costa Rica, 2009).

### Ministerio de Hacienda

*Sitio web: www.hacienda.go.cr*

Con una historia que se remonta a 1825, el Ministerio de Hacienda se creó formalmente en 1948 y fue reconocido como tal por la Constitución Política de Costa Rica de 1949. Está dividido en trece programas dirigidos a la ejecución de sus muchas responsabilidades. Este órgano administrativo es solo tangencialmente relacionado con el sector de las telecomunicaciones, ya que se encarga principalmente de dirigir el

[250] Este ministerio podría tener también algunas pequeñas responsabilidades repartidas a lo largo del marco normativo de las telecomunicaciones, como por ejemplo el determinar si las estaciones de radiodifusión califican como "cultural", que se encuentra en el artículo 97 de la Ley N º decreto reglamentario de 8642.

presupuesto público entrante hacia las diversas instituciones públicas, de acuerdo con el marco legal de nuestro país.

Uno de los ejemplos de esta participación puede ser encontrado en la administración temporal de la tasa del espectro radioeléctrico por la Dirección General de Tributación (uno de los programas de este ministerio), que según el artículo 173 del Decreto Ejecutivo N º 36774 -MINAET (Presidencia de la República de Costa Rica, 2011) será depositado posteriormente en las cuentas financieras de la SUTEL para ser ejecutado en el marco del Fondo Nacional de Telecomunicaciones (FONATEL ).

## Autoridades Administrativas y Regulatorias

Volviendo a la introducción del presente capítulo, el lector puede recordar que dada una serie de dificultades contextuales, Costa Rica adoptó un proceso de liberalización regulado y orientado por el Estado. Dicho proceso *"tiene la intención de garantizar una competencia efectiva, en pos de la transparencia del mercado, lo que se traduce en una beneficio directo para el usuario final de los servicios" (Poder Ejecutivo de la República de Costa Rica, 2009)*.

Como se indicó anteriormente, el marco legal vigente en Costa Rica para el sector de las telecomunicaciones determina al Estado, no solo como responsable de la rectoría del sector, sino que también le impone la obligación de crear entes independientes encargados de las tareas de regulación específicas al sector. Este deber se ha visto traducido en una reorganización del marco administrativo nacional dirigida a asegurar

que la administración pública pueda cumplir esta tarea de acuerdo con los requisitos de imparcialidad y de promoción de la libre competencia dentro del país.

Específicamente en materia de telecomunicaciones, vale la pena recalcar que tras la apertura del sector, algunas doctrinas tradicionalmente utilizadas en Costa Rica dejaron de ser compatibles con el sistema liberalizado previsto por la ley y los tratados internacionales relevantes (CAFTA-DR). Este es el caso de la consideración de las telecomunicaciones como un servicio público, línea doctrinal aplicada ampliamente durante la época de monopolio que (lastimosamente) debió ser sustituida por el concepto de "servicio a disposición del público" existente en la doctrina europea, el cual permite a los actores privados participar en la prestación de estos servicios sin estar sujetas al escrutinio excesivo y limitaciones características del régimen aplicable a los servicios públicos.

Esta diferenciación terminológica y doctrinaria tuvo también una repercusión clara en la manera en que es actualmente regulado el sector telecomunicaciones, pues al no ser los servicios de telecomunicaciones considerados como servicios públicos, no podrían ser regulados por la Autoridad Reguladora de los Servicios Públicos, sino que debió ser creado un nuevo ente especializado, desconcentrado e independiente[251] del Poder Ejecutivo: la Superintendencia de Telecomunicaciones.

Una vez hechas estas aclaraciones iniciales se procederá a estudiar las dos instituciones con que se cuenta actualmente para la regulación de las telecomunicaciones (ARESEP y SUTEL), a la vez que se mencionará también la Agencia

[251] Que por diversos motivos no fue creada como un ente totalmente independiente en nuestro país sino que, como veremos a continuación se constituye como un ente adjunto a la Autoridad Reguladora de los Servicios Públicos.

de Protección de Datos de los Habitantes, encargada únicamente de las tareas de fiscalización y regulación en materia de protección de datos personales.

### *Autoridad Reguladora de los Servicios Públicos*

Creada por la Ley Nº 7593 y reformada por la Ley Nº 8660, la Autoridad Reguladora de los Servicios Públicos (ARESEP) es una institución pública encargada de la tarea de regular los servicios públicos (tanto aquellos brindados por el Estado como aquellos sujetos a concesión).

Las principales funciones de esta autoridad son: la fijación de precios y tarifas, y el fungir como garante del cumplimiento de las normas de calidad, cantidad, confiabilidad, continuidad, oportunidad y rendimiento; para también procurar la armonización de los intereses de los consumidores, los usuarios y los proveedores de servicios públicos en el país[252]. Por otra parte, de acuerdo con las disposiciones de la Ley Nº 7593, la ARESEP se caracteriza por ser una institución autónoma del Estado, lo cual le da independencia administrativa completa del Poder Ejecutivo de acuerdo con los artículos constitucionales de Costa Rica 188-190[253].

Específicamente con respecto al sector de las telecomunicaciones, tanto las leyes N º 7593 y Nº 8660 establecen que las principales capacidades de la ARESEP son:

[252] Tales como: los servicios públicos de agua, servicios de saneamiento ambiental, servicios de electricidad, servicios de suministro de combustible y servicios de transporte. (Asamblea Legislativa de la República de Costa Rica, 1996).
[253] Estos artículos establecen la independencia administrativa de estas instituciones e imponen a la Asamblea Legislativa la obligación de escuchar la opinión de la institución al discutir y aprobar los proyectos relacionados con ella.

a) Ejecutar las funciones y cumplir sus deberes de acuerdo con lo dispuesto por el Plan Nacional de Desarrollo y los diversos planes de desarrollo sectoriales.
b) Dictar las políticas y normas dirigidas garantizar las condiciones de trabajo dentro de SUTEL y ARESEP.
c) Resolver los recursos contra las decisiones de la SUTEL sobre los precios y tarifas de servicios públicos, contribuciones, cánones, tasas y cánones.
d) Nombrar a los miembros de la Junta Directiva de la SUTEL.
e) Imponer sanciones y multas conforme con la ley.
f) Auditar las finanzas de la SUTEL.

Por último, se debe señalar que, de acuerdo con el apartado b del artículo 77 de la Ley Nº 8642, ARESEP se encuentra obligada a redactar y aprobar una serie de normas técnicas en relación con el mercado de las telecomunicaciones, las cuales incluyen los siguientes temas: acceso e interconexión; acceso universal y servicio universal; solidaridad; el régimen de protección al usuario final; prestación y calidad del servicio; régimen de competencia de las telecomunicaciones; precios y tarifas; encadenamiento de la red, transmisión y sincronización.

*Superintendencia de Telecomunicaciones*

Creada por la Ley N º 8660 del 13 de agosto 2008 como una agencia reguladora especializada para el sector de las telecomunicaciones recientemente liberalizado, la Superintendencia de Telecomunicaciones se constituye como un organismo de desconcentración máxima (solamente adscrito a la Autoridad Reguladora de los Servicios Públicos), que posee su propia personalidad jurídica e independencia de todos los proveedores de servicios y operadores de red del país.

Las principales actividades de la SUTEL se relacionan con la regulación, ejecución, seguimiento y control del marco legal específico aplicable al sector de las telecomunicaciones en el país, con el fin de garantizar la eficiencia, igualdad, continuidad, calidad, información y mejor cobertura de los sistemas de telecomunicaciones de Costa Rica.

En concreto, las responsabilidades de la SUTEL incluyen:

a) Aplicar el marco normativo de la nación para el sector de las telecomunicaciones.
b) Promover la diversidad de los servicios de telecomunicaciones y la introducción de nuevas tecnologías.
c) Garantizar y proteger los derechos de los usuarios finales.
d) Velar por que los operadores de redes y proveedores de servicios cumplan con sus obligaciones y asegurar sus derechos.
e) Asegurar, de manera objetiva, proporcional, oportuna, transparente, eficiente y no discriminatoria, el acceso a los escasos recursos relacionados con el funcionamiento de la red y la prestación de servicios de telecomunicaciones.
f) Controlar y asegurar el uso eficiente del espectro radioeléctrico; supervisar las emisiones radioeléctricas de la infraestructura de telecomunicaciones, tanto pública como privada en el país, y trabajar hacia la eliminación de las interferencias en el espectro.
g) Velar por que los operadores de redes dentro del país cumplan con las condiciones oficiales de las obligaciones de acceso de red , interoperabilidad de la red y de interconexión de redes.

h) Establecer y garantizar altos estándares de calidad para los servicios de red y de telecomunicaciones en el país y dirigir esas normas a maximizar la productividad y la eficiencia.

i) Garantizar la sostenibilidad del medio ambiente en las actividades que se relacionan con el sector.

j) Instruir y sancionar las infracciones administrativas derivadas de los operadores de redes y los proveedores de la red.

k) Proporcionar criterios técnicos para MICITT cuando sea necesario.

l) Administrar el Fondo Nacional de Telecomunicaciones del país (FONATEL) como un medio para la financiación y el desarrollo de proyectos dirigidos hacia el cumplimiento de los objetivos de servicio universal, acceso universal y de solidaridad incluidos en la Ley N º 8642 y el PNDT.

m) Establecer y administrar el Registro Nacional de Telecomunicaciones, dirigido a garantizar el acceso público a la información pertinente del sector (por ejemplo, concesiones, asignación de recursos, ofertas y acuerdos de interconexión, precios y tarifas, sanciones, reglamentos técnicos, acuerdos internacionales, otros).

n) Desarrollar, implementar, monitorear y controlar los reglamentos técnicos para el sector.

o) Procesar los títulos habilitantes para las empresas de telecomunicaciones, instruir el procedimiento de licitación, desarrollar los carteles de licitación y examinar las ofertas.

p) Garantizar su propia especialización técnica mediante la realización de actividades de capacitación para su personal y asegurar una estructura

institucional fuerte y moderna que permita el correcto funcionamiento del mercado de las telecomunicaciones.

q) Determinar si un proveedor de servicios u operador de red puede ser considerado un "operador importante" dentro de su respectivo mercado.

r) Gestionar un sistema fiable y actualizado de información sobre el estado actual de las telecomunicaciones en el país y de la penetración de las TIC en la sociedad costarricense.

s) Seguir las normas técnicas, económicas y jurídicas aplicables en materia de protección al usuario final de los servicios de telecomunicación, de conformidad con el capítulo II del título II de la Ley General de Telecomunicaciones. Esto incluye tramitar las reclamaciones originadas por la violación a los derechos de privacidad del usuario que establece dicha ley.

t) Denunciar ante el Ministerio Público toda responsabilidad penal en casos de violaciones a los derechos de los usuarios.

u) Coordinar audiencias públicas para la formulación y revisión de los reglamentos técnicos y los estándares aplicables al sector.

Finalmente, debe recalcarse que, en el contexto de nuestro marco jurídico actual, la SUTEL puede ser caracterizada como la agencia gubernamental que muestra la mayor participación en el proceso de normalización y estandarización de los sistemas de telecomunicaciones del país.

Así, el papel de la Superintendencia como un regulador para el sector, requerirá no solo el examen de las diversas prácticas y técnicas utilizadas por operadores de redes y proveedores de servicios, sino también el asegurar la continua actualización del marco

regulatorio del país. Para ello, la Superintendencia deberá prestar constante atención a las tendencias internacionales y los avances tecnológicos, para lograr incorporar estos a sus esfuerzos regulatorios (tanto legales como técnicos).

Finalmente, la fuerte relación de la SUTEL con el Viceministerio de Telecomunicaciones de MICITT le permitirá ofrecer su asesoramiento técnico y sus considerables fuentes de información al rector del sector, con miras a asegurar una correcta representación internacional del país y el desarrollo por parte de este último de políticas concordantes con las observaciones de la SUTEL.

### *Agencia de Protección de Datos de los Habitantes*

Creada por el artículo 15 de la Ley Nº 8968 del 7 de julio de 2011[254] y declarada su conformación "*de interés público y nacional*" por el Acuerdo Ejecutivo 212 de 22-11-2011, la Agencia de Protección de Datos de los Habitantes (PRODHAB) es un órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz cuyas atribuciones incluyen:

a) *"Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos;*
b) *Llevar un registro de las bases de datos reguladas por la ley 8968;*
c) *Requerir, de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados;*

[254] Lastimosamente, a casi tres años de promulgada esta ley y creada esta institución, la PRODHAB aún cuenta con una presencia muy limitada en nuestro país. Según la Directora Nacional de dicha institución, esta situación se ha relacionado fundamentalmente con una serie de limitaciones presupuestarias y administrativas que la agencia aún hoy procura solventar. (Artavia Chavarría, 2014).

*d) Acceder a las bases de datos reguladas por esta ley, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante la Agencia y, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información;*

*e) Resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales;*

*f) Ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y las bases de datos, cuando estas contravengan las normas sobre protección de los datos personales;*

*g) Imponer las sanciones establecidas, en el artículo 28 de esta ley, a las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos personales, y dar traslado al Ministerio Público de las que puedan configurar delito;*

*h) Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales;*

*i) Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial La Gaceta, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional;*

j) *Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales"* (Asamblea Legislativa de la República de Costa Rica, 2011).

Según la ley 8968, la PRODHAB cuenta con personalidad jurídica instrumental propia, lo cual le asegura tanto la capacidad para administrar sus recursos y presupuesto como la potestad de suscribir los contratos y convenios que requiera para el cumplimiento

de sus funciones, respecto de las cuales deberá también emplear procedimientos automatizados, de acuerdo con las mejores herramientas tecnológicas a su alcance.

### Operadores de Redes de Telecomunicaciones y Proveedores de Servicios

Los operadores de redes y proveedores de servicios[255] se reconocen como partes interesadas en el sector de telecomunicaciones de Costa Rica tanto por la Ley N º 8660 como por la Ley N º 8642 y son entendidos como una *"persona física o jurídica, pública o privada, que explota redes de telecomunicaciones con la debida concesión o autorización, las cuales podrán prestar o no servicios de telecomunicaciones disponibles al público en general"* (Asamblea Legislativa de la República de Costa Rica, 2008).

De acuerdo con esta definición, las concesiones[256] y autorizaciones[257] constituyen un requisito fundamental para los operadores de redes y los proveedores de servicios

[255] Actualmente el país tiene una larga lista de operadores de redes y proveedores de servicios, que van desde las instituciones públicas, como el ICE y RACSA, a los operadores de redes móviles privadas (Movistar, Claro), proveedores de servicios de red virtuales (Fullmóvil, VIVA, etc.) la telefonía IP proveedores (CALL MY WAY SA, RTI SA, TELE DIGA SA, etc.) y otros servicios. Dado que el estudio de la distribución específica de los servicios y las empresas que prestan esos servicios en el país supera los objetivos del presente estudio, me limitaré a remitir al lector a la lista completa de los proveedores de servicios que han recibido la autorización de la SUTEL hasta el mes de noviembre de 2013, véase: (Superintendencia de Telecomunicaciones, 2013).

[256] En el caso específico de las concesiones otorgadas en el contexto del sector de las telecomunicaciones, esta herramienta legal ha sido regulada por la Ley N º 8642 (artículos 11 a 22) que establece que "Se otorgará concesión para el uso y la explotación de las frecuencias del espectro radioeléctrico que se requieran para la operación y explotación de redes de telecomunicaciones. Dicha concesión habilitará a su titular para la operación y explotación de la red. Cuando se trate de redes públicas de telecomunicaciones, la concesión habilitará a su titular para la prestación de todo tipo de servicio de telecomunicaciones disponibles al público. La concesión se otorgará para un área de cobertura determinada, regional o nacional, de tal manera que se garantice la utilización eficiente del espectro radioeléctrico". (Asamblea Legislativa de la República de Costa Rica, 2008).

[257] También regulado por la Ley N º 8642, se requieren autorizaciones para aquellas personas físicas o jurídicas que "a) Operen y exploten redes públicas de telecomunicaciones que no requieran uso del espectro radioeléctrico. b) Presten servicios de telecomunicaciones disponibles al público por medio de redes públicas de telecomunicaciones que no se encuentren bajo su operación o explotación (...); y c)

(tanto públicos como privados) que operen en el país. En virtud de las disposiciones de la Ley Nº 8642, estos dos instrumentos jurídicos constituyen un requisito de entrada para cualquier persona interesada en el sector de las telecomunicaciones, y, como tales, imponen una serie de derechos y obligaciones a sus titulares, entre las cuales se encuentran[258]:

a) Operar las redes de telecomunicaciones y prestar servicios de acuerdo con las condiciones de su respectivo título habilitante y las demás disposiciones legales o técnicas aprobadas a tal efecto.
b) Cumplir con las obligaciones correspondientes al acceso universal, el servicio universal y las disposiciones en materia de solidaridad.
c) Respetar los derechos de los usuarios finales y manejar sus quejas conforme con la Ley .
d) Cumplir con los precios y tarifas dictadas por la SUTEL[259].
e) Registrar los servicios específicos que se proporcionan en la SUTEL en el Registro Nacional de las Telecomunicaciones y actualizar esta información antes de la entrega de cualquier nuevo servicio.

Operen redes privadas de telecomunicaciones que no requieran uso del espectro radioeléctrico". (Asamblea Legislativa de la República de Costa Rica, 2008).

[258] Se hace una excepción en el artículo 51 de la Ley N º 8642 para los proveedores de servicios de información, quienes están exentos de las responsabilidades de ofrecer sus servicios al público; justificar y registrar sus precios y tarifas conforme a sus costos; proporcionar acceso o la interconexión de sus redes; y de ajustarse a las normas o reglamentos técnicos para realizar interconexiones con redes privadas (deben sin embargo cumplir con dichas regulaciones cuando realicen de interconexiones con redes públicas de telecomunicaciones) (Asamblea Legislativa de la República de Costa Rica, 2008).

[259] De acuerdo con el artículo 50 de la Ley Nº 8660, la SUTEL fijará inicialmente los precios y tarifas del sector telecomunicaciones, y continuará haciéndolo hasta que determine que el país se ha reunido un número suficiente de condiciones que garanticen una competencia leal y efectiva del mercado. Una vez se cumpla dicho requisito los precios y tarifas quedarán a disposición de los proveedores de servicios conforme a los requerimientos del mercado. (Asamblea Legislativa de la República de Costa Rica, 2008).

f) Diseñar sus redes públicas de acuerdo con las condiciones técnicas, jurídicas y económicas que aseguren su interoperabilidad.
g) Presentar a la SUTEL cualquier informe solicitado o la documentación con las condiciones y periodicidad que se determine.
h) Garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos de carácter personal de los abonados y usuarios finales mediante la implementación de los sistemas y las medidas técnicas y administrativas necesarias idóneas para garantizar la seguridad de las redes y sus servicios.
i) Informar a la SUTEL y a los usuarios en caso de que sea identificado un peligro para la red o los datos de los usuarios.
j) Eliminar o anonimizar los datos de tráfico y localización relacionados con los usuarios finales, que sean tratados y almacenados bajo la responsabilidad de un operador o proveedor cuando no sean necesarios para la facturación o transmisión de una comunicación.

En el caso específico de los "operadores importantes"[260] estas responsabilidades también incluyen:

a) Dar a conocer de forma clara, suficiente, completa y exacta toda la información solicitada por la SUTEL.
b) Mantener procesos separados para la contabilidad de los costos de sus servicios de acuerdo con las normas técnicas aplicables.

[260] Dentro de esta clasificación actualmente solo se encuentra el Instituto Costarricense de Electricidad, institución que con base en las disposiciones de la Ley Nº 8660 actualmente brinda sus servicios en competencia.

c) Abstenerse de incurrir en prácticas monopólicas.

d) Someterse a las tarifas y los aranceles correspondientes.

e) Prestar servicios y acceso a otros operadores y usuarios de la misma calidad que aquellos proporcionados a sus propios abonados.

Una vez considerados todos estos puntos no puede haber ninguna duda de que, de acuerdo con el marco legal de las telecomunicaciones en Costa Rica, los operadores de redes y proveedores de servicios asumen nuevas responsabilidades, incluso después de haber cumplido plenamente los requisitos iniciales para obtener la concesión o autorización requerida para ofrecer sus servicios al público.

Concretamente, debe señalarse que dichos actores se encontrarán obligados a adoptar una serie de acciones dirigidas a la consecución de las metas y objetivos de que, en el caso del PNDT (2009-2014) vigente, se encuentran plasmadas en la línea estratégica "redes y sistemas de telecomunicaciones", pero que futuras versiones de dicho plan podrán ampliar o reducir conforme se considere necesario.

Por último, debe tenerse en cuenta que de acuerdo con el marco normativo aplicable y el eje de telecomunicaciones del PNDT, los operadores de redes y proveedores de servicios tienen el derecho y la responsabilidad de introducir servicios innovadores (y especialmente convergentes) a sus redes [261] e iniciar la unificación de las

[261] De acuerdo con el artículo 27 de la Ley Nº 8642, la introducción de nuevos servicios a una red de telecomunicaciones no requiere que el operador o proveedor de servicio solicite una nueva concesión o autorización, ya que el único requisito para la prestación de servicios adicionales para el público es que dichos operadores le informen previamente a SUTEL y cumplan con aquellas peticiones mediante las cuales SUTEL solicite más información o requiera realizar los ajustes necesarios para garantizar que el nuevo servicio cumple con los estándares regulatorios correspondientes. (Asamblea Legislativa de la República de Costa Rica, 2008).

telecomunicaciones de voz con protocolos digitales, tales como VoIP[262]. Esta situación ha llevado a la mayoría de los grupos de interés a brindar sus propios servicios o a animar a sus usuarios a adoptar los servicios, proporcionados por proveedores de servicios de internet nacionales o internacionales disponibles de forma libre y gratuita, *"que el usuario puede activar en cualquier momento"* (MINAET - Viceministerio de Telecomunicaciones, 2012, pág. 82).

[262] Esto ha sido señalado específicamente por el eje de telecomunicaciones del PNDT dentro de su línea de acción k), la cual procura "unificar las telecomunicaciones de voz hacia protocolos digitales (IP inicialmente y su evolución" y a continuación establece dos metas específicas: 1) asegurar que al menos tres proveedores brinden servicios de VoIP para mayo del 2010 y 2) lograr que el 100% de los proveedores de Internet (ISP) brinden servicios de voz digital. (MINAET - Viceministerio de Telecomunicaciones, 2012, pág. 82) .
Lastimosamente, a pesar de que ambas metas han sido marcadas como cumplidas por el Viceministerio de Telecomunicaciones, la realidad es que los operadores y proveedores se han limitado a incentivar en sus usuarios la adopción de tecnologías convergentes brindadas por terceras partes (usualmente empresas basadas en otros países tales como Microsoft, Apple, etc.), lo cual no hace más que incentivar los problemas de la protección de datos personales y la transferencia transfronteriza de datos.

### *Síntesis de la Primera Sección*

*A lo largo de la cual se analiza tanto el marco histórico y contextual de la evolución de las telecomunicaciones en Costa Rica como el marco administrativo que las rodea y las coordina.*

- Costa Rica presenta un contexto muy apto para el desarrollo del mercado de las telecomunicaciones. No solamente cuenta con altos índices de desarrollo y de adopción de tecnologías de la información, sino que presenta también una larga historia de estabilidad política y económica.
- Esta estabilidad se encuentra basada en la historia del país, la cual permitió la instauración de un Estado de Derecho basado en políticas de bienestar que dirigieron la historia del país desde 1949 hasta inicios de la década de 1980.
- Durante estas tres décadas ocurrieron en nuestro país grandes ejemplos de progreso. Específicamente relevante para la materia en estudio es la fundación del Instituto Costarricense de Electricidad y las grandes inversiones realizadas por esta institución con miras a popularizar el acceso a las telecomunicaciones por el país.
- A partir de la década de los 80, el cambio en el modelo económico imperante dirige a los países del mundo hacia la adopción de políticas neoliberales. Dichas políticas son adoptadas también por Costa Rica (por medio de los Programas de Reajuste Estructural) y con ello inicia el impulso gubernamental hacia la privatización / apertura del mercado de las telecomunicaciones.
- A pesar de ello, las décadas de los 80 y 90 conllevan también grandes ejemplos de progreso para el sector de telecomunicaciones del país; ejemplo de lo cual es la conexión del país a las redes mundiales de telecomunicaciones y la oferta al público del acceso a internet.
- La llegada del nuevo milenio trae consigo una época de gran cambio en materia de telecomunicaciones para Costa Rica. El gobierno intenta aprobar el “Combo del ICE” y al ver fallidos sus intentos dirige su atención hacia la negociación del CAFTA-DR.

- Tras un referéndum, es aprobada la apertura del mercado de las telecomunicaciones en Costa Rica; como parte de las responsabilidades adoptadas por el Estado, son aprobadas una serie de leyes complementarias al tratado de libre comercio que producen una serie de cambios estructurales importantes, dentro de las que destacan la Ley Nº 8660 y la Ley Nº 8642.
- El nuevo panorama de las telecomunicaciones en Costa Rica se encuentra marcado por un Estado que adopta un rol triple: rector, regulador y operador.
- Dentro de este nuevo panorama, el rol de *rector* es adoptado por el Presidente de la República y su Ministro de Ciencia, Tecnología y Telecomunicaciones, quien dirige el ministerio del mismo nombre y es apoyado por el Viceministerio de Telecomunicaciones.
- CAFTA-DR requiere que nuestro país cree un ente independiente encargado de las funciones de *regulación* para el sector. Así es creada la Superintendencia de Telecomunicaciones por la Ley 8660 como ente adscrito a la Autoridad Reguladora de Servicios Públicos.
- En Costa Rica los servicios de telecomunicaciones no son ya considerados Servicios Públicos; actualmente se sigue la doctrina de que estos son “Servicios disponibles al público”.
- El Instituto Costarricense de Electricidad, que antiguamente asumió la dirección de las telecomunicaciones en el país e incluso lo representaba ante entes internacionales especializados, actualmente es considerado el único *operador* Importante del país y opera sus redes en el mercado junto con los otros operadores de telecomunicaciones.
- Los operadores de redes y los proveedores de servicios requieren de autorizaciones o concesiones para brindar sus servicios al público. Dichas autorizaciones y concesiones conllevan una carga importante de responsabilidades y derechos, que incluyen aquellas impuestas sobre dichos actores por el Plan Nacional de Desarrollo de las Telecomunicaciones.
- Los operadores y proveedores son activamente incentivados por el PNDT a brindar servicios convergentes a sus usuarios. Para ello solamente requieren informar previamente a SUTEL de los servicios nuevos por brindar y cumplir,

con los requisitos técnicos que esta autoridad imponga para los nuevos servicios.

## Sección II: Marco Regulatorio Vigente en Costa Rica en Materia de Telecomunicaciones y Protección de Datos Personales

A lo largo de la presente sección se habrá de examinar el marco regulatorio vigente en Costa Rica, con miras a comprender el conjunto de obligaciones que dirigen actualmente a los diversos actores del sector de telecomunicaciones. Asimismo, se estudiará la legislación nacional e internacional aplicables en nuestro país en materia de protección de datos personales, con un enfoque especialmente para ello, en aquellas disposiciones relevantes a las telecomunicaciones convergentes.

## *Marco Regulatorio Vigente en Materia de Telecomunicaciones*

Una vez concluido el estudio de los antecedentes históricos y administrativos del sector de telecomunicaciones de Costa Rica, se centrarán esfuerzos en la comprensión de las complejidades del marco legal que regula este sector en el país. Para ello, se dedicará tiempo a explorar las normas nacionales e internacionales que pueden resultar relevantes para este sector, procurando enfocar la atención especialmente en aquellos instrumentos legales que posean alguna relevancia para la protección de datos en el país.

## Tratados Internacionales Ratificados por la República de Costa Rica en Materia de Telecomunicaciones

Los acuerdos internacionales se han convertido en herramientas importantes en el mundo globalizado de las telecomunicaciones. No solo permiten a diversos países formalizar acuerdos y unificar posiciones sobre asuntos importantes, sino que también tienden a generar el contexto necesario sobre el cual se basan las leyes nacionales y los reglamentos técnicos.

Como se indicó anteriormente, Costa Rica debe su mercado de telecomunicaciones liberalizado a un acuerdo internacional de libre comercio (CAFTA-DR), que también introdujo elementos reguladores modernos para el marco administrativo de nuestro país. Por otra parte, el país ha sido un miembro de larga data de varias organizaciones internacionales relacionadas con las telecomunicaciones, y esto ha dado lugar a una gran aceptación de la legitimidad de sus acuerdos, normas y recomendaciones, las cuales han sido incorporadas fácilmente en la normativa local y las prácticas técnicas.

Hasta inicios de 2014, Costa Rica ha ratificado al menos diez acuerdos y tratados internacionales que se relacionan directamente con el sector de las telecomunicaciones, a saber:

### *Convención Internacional de Telecomunicaciones*

Instrumento esencial de la Unión Internacional de Telecomunicaciones, el Convenio Internacional de Telecomunicaciones ha sido ratificado en tres ocasiones por la República de Costa Rica. Específicamente, nuestro país ratificó la convención por primera vez el día 07 Octubre de 1963, con la aprobación de la Ley Nº 3193; posteriormente, la Ley N º 5233 ratificó la convención de Montreux de 1965 el 09 de julio de 1973 y, finalmente, la Ley Nº 6347 ratificó el Convenio de Málaga - Torremolinos de 1973, el día 03 de septiembre de 1979.

Los objetivos fundamentales de este acuerdo se dirigen a "*preservar y ampliar la cooperación internacional para el mejoramiento y el empleo racional de las telecomunicaciones de todo tipo, que favorece el desarrollo de los medios técnicos y garantizar su funcionamiento eficaz con el fin de aumentar el rendimiento de los servicios de telecomunicaciones, así como su utilidad y uso generalizado del público y, finalmente, armonizar las actividades nacionales para el logro de estos fines*" (MINAET - Viceministerio de Telecomunicaciones, 2009).

Estos tres acuerdos introdujeron oficialmente a Costa Rica ante la Unión Internacional de Telecomunicaciones, por lo que su ratificación por el país representa la aceptación de su papel como un participante activo en las conferencias y comités consultivos de la Unión. Por último, se debe recordar que la Convención requiere que nuestro país siga y adopte las directivas, directrices y recomendaciones de normalización y estandarización generadas por la UIT.

### *Constitución y Convención de la Unión Internacional de las Telecomunicaciones*

La Constitución y el Convenio de la UIT se aprobaron en 1992 en Ginebra y posteriormente fueron ratificados (junto con las enmiendas que se generan en la Conferencia Plenipotenciaria de 1994 en Kyoto) por el Estado de Costa Rica mediante la Ley N º 8100 el 08 de abril de 2002.

El Convenio extiende los fines de la UIT, adoptando como fundamentales los siguientes objetivos:

a) Mantener y ampliar la cooperación internacional entre todos los Estados Miembros de la UIT para el mejoramiento y el empleo racional de toda clase de telecomunicaciones.
b) Promover y brindar asistencia técnica a los países en desarrollo en el ámbito de las telecomunicaciones y promover la movilización de recursos materiales y financieros necesarios para su ejecución.
c) Promover el desarrollo de los medios técnicos y su más eficaz explotación, a fin de aumentar el rendimiento de los servicios de telecomunicaciones, acrecentar su empleo y generalizar lo posible su utilización por el público.
d) Promover la extensión de los beneficios de las nuevas tecnologías de telecomunicaciones a todos los habitantes del planeta.
e) Promover la utilización de los servicios de telecomunicaciones con el fin de facilitar las relaciones pacíficas.
f) Armonizar los esfuerzos de los miembros para alcanzar estos fines.
g) Promover la adopción internacional de un enfoque más amplio de las cuestiones de telecomunicaciones, teniendo en cuenta la globalización de la economía y la sociedad de la información, mediante la cooperación con otras

organizaciones intergubernamentales y organizaciones no gubernamentales mundiales y regionales interesadas en las telecomunicaciones.

Al firmar y ratificar este convenio Costa Rica adoptó todas estas metas; sin embargo, debe tenerse en cuenta que durante la Conferencia Plenipotenciaria de Kyoto de 1994, los representantes de Costa Rica presentaron tanto reservas como declaraciones, según las cuales:

*"La delegación de Costa Rica a la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones:*

*1. Reserva para su Gobierno el derecho de:*

*a) Tomar las medidas que considere necesarias para proteger sus intereses nacionales y sus servicios de telecomunicaciones, que otros Miembros dejen de cumplir las disposiciones de las Actas Finales de esta Conferencia (Kioto, 1994).*

*b) Adoptar las reservas que considere necesarias antes de la ratificación de las Actas Finales de la presente Conferencia en relación con las disposiciones de los actos finales que puedan infringir la Constitución de Costa Rica.*

*2. Declara que Costa Rica estará obligado por los instrumentos de la Unión Internacional de Telecomunicaciones , que comprende la Constitución, el Convenio , los Reglamentos Administrativos y las enmiendas o modificaciones a los mismos solamente cuando significa explícitamente su consentimiento en obligarse por cada uno de esos instrumentos y condicionadas a la previa de sus procedimientos constitucionales pertinentes"* (International Telecommunications Union, 1994).

### *Tratado Centroamericano de Telecomunicaciones y su Protocolo*

Ratificado por Ley N º 4031 el 23 de diciembre 1967 (Asamblea Legislativa de la República de Costa Rica, 1967), este tratado se complementó con la firma y la ratificación de su protocolo por la Ley N º 8209 el 31 de mayo de 2002 (Asamblea Legislativa de la República de Costa Rica, 2002). En concreto, este tratado propone la construcción y el uso conjunto de una red regional de telecomunicaciones que una las capitales de América Central y facilite las comunicaciones regionales.

### *Acuerdo Relacionado con la Organización Internacional de Telecomunicaciones por Satélite*

Ratificado por Ley N º 4806 el 28 de julio 1971 (Asamblea Legislativa de la República de Costa Rica, 1971). Este acuerdo crea la Organización Internacional de Telecomunicaciones por Satélite como una organización intergubernamental que apoya el principio establecido en la Resolución 1721 (VI) de las Naciones Unidas. Para ello pretende que las comunicaciones por satélite se encuentren a disposición de las naciones del mundo de una manera no discriminatoria.

Los principios fundamentales de esta organización son:

a) Mantener una conectividad mundial y una cobertura global.
b) Brindar a sus clientes conectividad vital.
c) Facilitar el acceso a su sistema de manera no discriminatoria.

### *Convención Internacional de Telecomunicaciones Marítimas por Satélite*

Ratificado por Ley N º 7486 del 28 de marzo de 1995 (Asamblea Legislativa de la República de Costa Rica, 1995), este convenio establece la Organización Internacional de Telecomunicaciones Marítimas por Satélite, cuyo objetivo es perfeccionar las telecomunicaciones marítimas y aeronáuticas como medio para garantizar la emergencia y de la seguridad de las telecomunicaciones. Como signatario de la Convención, Costa Rica se compromete a contribuir en función de su participación en la organización.

### *Tratado Centroamericano de Libre Comercio e Integración Económica*

Acuerdo de libre comercio firmado por los países de América Central y ratificado por la Ley N º 3146 del 29 de julio 1963; tiene como objetivo fortalecer e integrar las economías de la región mediante el establecimiento de un régimen de comercio estable y claro entre los países firmantes. Asimismo, procura este tratado lograr el establecimiento de las disposiciones fundamentales en temas clave, como lo son las prácticas discriminatorias, el libre tránsito de mercancías, las subvenciones de exportación, la inversión extranjera, la integración industrial, el transporte regional y las telecomunicaciones.

En materia de telecomunicaciones, los miembros firmantes se comprometieron a *"mejorar los sistemas de telecomunicaciones entre sus respectivos territorios y unir sus esfuerzos hacia el logro de este propósito"* (Asamblea Legislativa de la República de Costa Rica, 1963).

### *Acuerdo Marco de Cooperación entre las Repúblicas de Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá y la Comunidad Económica Europea.*

Suscrito el 22 de febrero de 1993 y ratificado por la Ley N º 7616 el 04 de septiembre de 1996, este convenio revisa diversos tipos de cooperación (sobre todo en las materias económicas, tecnológicas, industrial y de regulación) con el fin de mejorar el desarrollo regional. El artículo 16 del acuerdo se refiere específicamente al sector de las telecomunicaciones, y establece que:

*"Artículo 16: La cooperación en el campo de la tecnología de la información y las telecomunicaciones*

1- *Las Partes Contratantes reconocen que la tecnología de la información y las telecomunicaciones son particularmente importantes para el desarrollo económico y social , se declaran dispuestas a impulsar la cooperación en áreas de interés común , en particular en lo que respecta a:*

   *- La promoción de las inversiones y las empresas mixtas;*

   *- Normalización, pruebas de conformidad y la certificación;*

*- Sistemas Rurales y la telefonía móvil, así como la tierra y el espacio, como las redes de transporte de telecomunicaciones, satélites, fibra óptica, redes digitales de servicios integrados (RDSI) y transmisión de datos;*

*- Electrónica y microelectrónica;*

*- La informatización y la automatización;*

*- Investigación y desarrollo de nuevas tecnologías de la información y las telecomunicaciones.*

2- *Esta cooperación se realizará en particular mediante :*

*- La promoción de proyectos conjuntos de investigación y desarrollo y la creación de redes de información y bases de datos y el acceso a los bancos y las redes existentes;*

*- La colaboración entre los expertos;*

*- Evaluaciones de expertos, estudios e intercambios de información;*

*- La formación de personal científico y técnico;*

*- La definición y ejecución de proyectos de interés común"* (Asamblea Legislativa de la República de Costa Rica, 1996).

## *Declaración Conjunta entre los Gobiernos de Canadá y Costa Rica sobre Comercio Electrónico Global*

Dada durante el proceso de implementación del Tratado de Libre Comercio entre Costa Rica y Canadá, la Declaración Conjunta sobre Comercio Electrónico Global respondió a la necesidad de maximizar los esfuerzos internacionales encaminados a fortalecer el comercio electrónico, como motor de la innovación y el progreso.

Esta declaración conjunta se basó en cinco principios generales compartidos entre las dos naciones, a saber:

1. *"La creación de confianza para los usuarios y consumidores - que garanticen medidas de seguridad para ofrecer protección y aumentar la confianza en el mercado digital , abordando cuestiones tales como la privacidad, la seguridad y la protección del consumidor;*
2. *Establecer reglas de juego objetivas y transparentes para el mercado – reconociendo que los marcos jurídicos y comerciales existentes en áreas como el derecho contractual y la propiedad intelectual se aplican a las transmisiones electrónicas y tomen en cuenta el crecimiento futuro del comercio electrónico y su potencial social digital.*
3. *Mejora de la infraestructura de información que asegure el acceso efectivo a bajo costo, las redes de telecomunicaciones de alta calidad y servicios para el comercio electrónico;*
4. *Maximizar los beneficios - abordando las necesidades de las empresas, incluidas las pequeñas y medianas empresas (PYME), las organizaciones y los consumidores en el desarrollo y los países desarrollados sociales y económicos;*
5. *Promoción de la participación mundial en desarrollo de un enfoque de colaboración amplia que incluya a los gobiernos, el sector privado, la comunidad en general, las organizaciones internacionales que tenga por objeto maximizar el potencial social y económico del comercio electrónico en todas las economías y las sociedades"* (Gobiernos de Costa Rica y Canadá, 2001)

Adicionalmente, la declaración dedica una sección específica a las normas técnicas, a lo largo de la cual establece que: *"Los dos países apoyan la labor realizada por diversas organizaciones internacionales, como la Organización Internacional de Normalización (ISO), la*

*Unión Internacional de Telecomunicaciones (UIT) y la CITEL en el trabajo hacia estándares abiertos, interoperables, confiables y compatibles. Estas normas deberán estar dirigidas por el mercado basarse en el principio de la neutralidad tecnológica"* (Gobiernos de Costa Rica y Canadá, 2001).

### *Tratado de Libre Comercio entre Estados Unidos, Centroamérica y República Dominicana*

Como se dijo anteriormente, el Tratado de Libre Comercio entre Estados Unidos, Centroamérica y República Dominicana fue el punto de inflexión para el proceso de liberalización de las telecomunicaciones en Costa Rica. Ratificado por Ley N º 8622 el 21 de diciembre de 2007, este importante acuerdo comercial detalla los términos y condiciones para un nuevo marco de comercio multilateral entre las partes firmantes.

En concreto, el CAFTA-DR incluye disposiciones sobre las cuestiones relacionadas con temas como el comercio transfronterizo de servicios, los servicios financieros, la inversión, las compras del sector público, el acceso a mercados, agricultura, los derechos de propiedad intelectual, las medidas *antidumping*, la solución de controversias, la protección del medio ambiente, las normas laborales, la transparencia, la exclusividad de datos de prueba y las telecomunicaciones.

El capítulo decimotercero del DR -CAFTA establece una serie de acuerdos relevantes al sector de las telecomunicaciones. Frente a este contexto, el gobierno de Costa Rica negoció los términos específicos en los que esta sección del acuerdo sería implementada en el país. Los resultados de estas negociaciones fueron incorporadas al

tratado como anexo 13 al capítulo. Mediante el título "*Compromisos Específicos de Costa Rica sobre los Servicios de Telecomunicaciones*", en este anexo se reconoce la naturaleza única de la política social de Costa Rica en materia de telecomunicaciones y se emprende una serie de compromisos , que incluyen:

a) La modernización del ICE.
b) La aplicación de una serie de compromisos selectivos y graduales de apertura del mercado.
c) La adopción de una serie de principios reguladores (servicio universal, independencia de la autoridad reguladora, transparencia, asignación y utilización de recursos escasos, interconexión regulada, acceso y uso de la red, prestación de servicios de información, competencia, sistemas de cables submarinos y flexibilidad en la elección de las tecnologías).

La ratificación del CAFTA-DR es indudablemente relevante para la presente investigación dado que ha sido fundamental para la creación del sector telecomunicaciones actual de nuestro país. Asimismo, se debe resaltar que las disposiciones encontradas en CAFTA-DR no solamente se han visto traducidas en el marco legal actual costarricense, sino que han dirigido gran parte de las políticas adoptadas por SUTEL hasta la fecha.

## Normativa Nacional en Materia de Telecomunicaciones

Como se dijo anteriormente, el marco regulatorio actual de Costa Rica para el sector de las telecomunicaciones se ha desarrollado principalmente como parte de la agenda de implementación del CAFTA-DR, cuya ratificación tardía requirió de nuestro país la adopción de un ritmo rápido para la elaboración y adopción de la legislación nacional (y de la reglamentación técnica) necesaria para asegurar el cumplimiento del país con las obligaciones adquiridas con sus nuevos socios comerciales.

La legislación de telecomunicaciones actual se centra principalmente en dos leyes fundamentales (la Ley N º 8660 y la Ley N º 8642), que no solo han determinado las características generales del sector de las telecomunicaciones, sino que también han servido para modificar algunas leyes de larga data relacionadas con las telecomunicaciones del país.

Considerando lo anterior, se examinará de manera más detallada alguna de la normativa nacional más relevante para el sector telecomunicaciones en la actualidad.

### *Ley Nº 8660 "Ley de Fortalecimiento y Modernización de las Entidades Públicas"*

Aprobada por la Asamblea Legislativa de Costa Rica el 29 de julio de 2008, la Ley Nº 8660 sobre el fortalecimiento y modernización de las entidades públicas del sector telecomunicaciones constituye uno de los pasos fundamentales hacia el cumplimiento del país con las disposiciones del DR- CAFTA.

En su forma actual, la Ley N º 8660 no solamente incluye las disposiciones elementales para la creación del sector de las telecomunicaciones de la nación y "moderniza y

fortalece" tanto al ICE como a sus empresas; sino que también amplía y regula las competencias y atribuciones del Ministerio de Ciencia, Tecnología y Telecomunicaciones, a la vez que modifica la ley N º 7593 con el fin de crear la SUTEL en el marco administrativo de la ARESEP.

En concreto, la Ley N º 8660 cubre los siguientes temas:

a) Establece una serie de objetivos fundamentales, dentro de los cuales menciona específicamente tanto la rectoría del ministro del sector, como las responsabilidades de la SUTEL como regulador, ejecutor, monitor y controlador del marco regulador de las telecomunicaciones en el país.
b) Establece los principios rectores anteriormente mencionados para todas las entidades públicas que se relacionan con el sector de las telecomunicaciones (universalidad, solidaridad, beneficio del usuario, transparencia, competencia efectiva, no discriminación, neutralidad tecnológica, optimización de recursos escasos, privacidad de la información y sostenibilidad del medio ambiente).
c) Reconoce el papel del ICE como una institución autónoma del Estado y permite su funcionamiento en el mercado liberalizado mediante el establecimiento de una serie de disposiciones administrativas relativas a las nuevas capacidades de la institución (que ahora incluyen el suministro de servicios de información convergentes, así como el establecimiento de cualquier tipo de acuerdos y asociaciones con organizaciones nacionales e instituciones internacionales).

d) No incluye los servicios de telefonía tradicionales [263] del proceso de liberalización, pero permite a la SUTEL regular el servicio.

e) Declara la información de los usuarios y clientes del ICE como confidencial y proporciona el mismo estatus a cualquier información que la institución determine como un secreto industrial, comercial o económico no apto para su divulgación a terceros.

f) Determina las tareas del Ministro de Ciencia, Tecnología y Telecomunicaciones como rector del sector.

g) Constituye el Plan de Desarrollo Nacional de Telecomunicaciones como la herramienta más importante para la planificación y la orientación sectorial, que debe tener en cuenta tanto las políticas nacionales como los compromisos internacionales que han sido ratificados por el país;

h) Declara las responsabilidades de ARESEP, incluyendo su participación en el proceso de reglamentación técnica para los servicios públicos "de acuerdo con las normas específicas disponibles en el país o en el extranjero".

i) Crea SUTEL y establece sus responsabilidades, incluyendo su obligación fundamental de *"establecer y asegurar los estándares de calidad para las redes y servicios de telecomunicaciones para que sean más eficientes y productivos"* [264] (Asamblea Legislativa de la República de Costa Rica, 2008).

[263] Definidos por la Ley Nº 8660 como "el que tiene como objeto la comunicación de usuarios, mediante centrales de conmutación de circuitos para voz y datos, en una red predominantemente alámbrica, con acceso generalizado a la población; se excluyen los servicios de valor agregado asociados" (Asamblea Legislativa de la República de Costa Rica, 2008).

[264] Los incisos k) y r) del artículo 73) de esta ley declaran que esta tarea es responsabilidad conjunta de la junta directiva de SUTEL y la ARESEP, quienes deberán proponer los reglamentos técnicos al Poder Ejecutivo para su eventual aprobación.

j) Determina las responsabilidades específicas de los operadores de redes y proveedores de servicios.

k) Crea el Registro Nacional de Telecomunicaciones donde SUTEL debe registrar y publicar (entre otros temas) la legislación nacional e internacional para el sector, las normas y estándares de calidad, los reglamentos técnicos, los acuerdos técnicos privados y cualquier otro evento o acto que se torne relevante para el bienestar del sector.

Considerando todo esto, resulta evidente que la Ley N º 8660 no solamente es una piedra angular del proceso de liberalización, sino que también se convierte en una parte fundamental del marco legislativo nacional al asignar de manera clara las responsabilidades sobre la creación de regulaciones técnicas y estandarización, las cuales finalmente marcan las políticas de privacidad y protección del usuario en el sector.

*Reglamento al Título II de la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones*

Aprobado mediante decreto ejecutivo Nº 35148-MINAET del 24 de febrero de 2009, este reglamento procura reglamentar los alcances relevantes a las nuevas capacidades del ICE en el mercado liberalizado y determinar de manera exacta su relación con respecto la legislación administrativa en materia de contratación administrativa.

Para ello, el reglamento examina una serie de temas dentro de los cuales se encuentran la aptitud necesaria para contratar con la administración, el cartel de la licitación, los elementos básicos de la oferta, las modalidades de la licitación (pública, abreviada, con financiamiento, con precalificación, entre otros), los medios electrónicos de contratación administrativa, los tipos de contratos, y otros.

Es necesario recalcar que este reglamento presenta una particularidad importante para la presente investigación: uno de sus artículos contiene una potencial violación a la protección de datos personales. Se trata del artículo 9º del reglamento, el cual asigna al ICE la potestad de vender información de sus clientes y que reza:

*"Artículo 9º—**El ICE definirá los procedimientos para compartir la información que obtengan de sus clientes para los fines exclusivos del negocio, pero con resguardo de los derechos de los usuarios, y según lo establecido en la Ley general de telecomunicaciones y su reglamento.** Podrá asimismo establecer las políticas, procedimientos y acciones, generales y específicos, que consideren convenientes para proteger la información calificada como secreto comercial, industrial o económico, quedando facultados para suscribir contratos de confidencialidad con sus empleados, proveedores, socios o aliados estratégicos y cualquier otra persona o tercero interesado. No podrá el ICE y sus empresas negarse a suministrar, sin reserva o condicionamiento alguno, al Ministerio de Ambiente, Energía y Telecomunicaciones, Autoridad Reguladora de los Servicios Públicos, Superintendencia General de Telecomunicaciones, Contraloría General de la República u otros órganos públicos, aquella información que por Constitución o ley esas instancias pueden requerir.*

*El ICE, de conformidad con los artículos 9º y 10 de la Ley Nº 8660 y por razones de oportunidad y conveniencia comercial, y con respeto a la Ley general de telecomunicaciones, **podrá vender información no calificada en los términos señalados en primer párrafo de este artículo, según***

***las condiciones del mercado. Los procedimientos para la clasificación, custodia, administración y venta información comprenderán los propios del ICE y los de sus empresas***" [El subrayado no es del original] (Poder Ejecutivo de la República de Costa Rica, 2009).

### *Ley Nº 8642 "Ley General de Telecomunicaciones"*

Constituyéndose como la segunda piedra angular del marco actual de las telecomunicaciones de Costa Rica, nuestra Ley N º 8642: Ley General de Telecomunicaciones, fue aprobada el 4 de junio de 2008 por la Asamblea Legislativa como la nueva columna vertebral del recién liberalizado sector de las telecomunicaciones.

Esta ley expande la labor realizada por la Ley N º 8660 y establece el alcance y los mecanismos de regulación de las telecomunicaciones del país. Para ello, la Ley declara una serie de objetivos elementales y asume el mismo conjunto fundamental de principios que la Ley N º 8660.

La Ley General de Telecomunicaciones cubre un gran número de temas, dentro de los cuales, las disposiciones más relevantes para los fines de esta investigación son:

a) Aclara la diferencia existente entre los servicios de telecomunicaciones[265] y los servicios de información[266] y excluye estos últimos del ámbito de control de

[265] Definidos por el inciso 23 del artículo 6 de la ley Nº 8642 como aquellos *"servicios que consisten, en su totalidad o principalmente, en el transporte de señales a través de redes de telecomunicaciones. Incluyen los servicios de telecomunicaciones que se prestan por las redes utilizadas para la radiodifusión sonora o televisiva. (Asamblea Legislativa de la República de Costa Rica, 2008).*

SUTEL, reservándose únicamente la posibilidad de imponer ciertas obligaciones para corregir prácticas monopólicas, promover la competencia o resguardar los derechos de los usuarios por medio de su artículo 51.

b) Confirma el espectro radioeléctrico como bien público e impone al Poder Ejecutivo la responsabilidad de crear un plan de atribución nacional de frecuencias (para lo cual este deberá considerar las recomendaciones de la UIT y de la CITEL).

c) Establece los procedimientos específicos para todos los títulos habilitantes reconocidos en nuestro país (concesiones, autorizaciones y permisos).

d) Prohíbe cualquier concesión o autorización relacionada con los servicios de telefonía pública básica.

e) Permite a los operadores de redes y a los proveedores de servicios la introducción de nuevos servicios a sus redes sin necesidad de nuevos títulos habilitantes.

f) Relega las transmisiones unidireccionales de radiodifusión y televisión a las disposiciones de la Ley N º 1758 "Ley de Radio" de 19 de junio 1954, pero declara que cada vez que las emisoras se tornen tecnológicamente capaces de proporcionar servicios de telecomunicaciones a través de sus redes deberán ajustarse a las disposiciones de la Ley N º 8642.

g) Declara que cualquier operador de sistema de satélites deberá cumplir con los requisitos específicos de la concesión y se debe *"a) conformar sus transmisiones a*

[266] Definidos por la Ley Nº 8642 en el inciso 25 de su artículo sexto como aquel servicio que *"permite generar, adquirir, almacenar, recuperar, transformar, procesar, utilizar, diseminar, o hacer disponible información, incluso la publicidad electrónica, a través de las telecomunicaciones. No incluye la operación de redes de telecomunicaciones o la prestación de un servicio de telecomunicaciones propiamente dicha" (Asamblea Legislativa de la República de Costa Rica, 2008).*

*la UIT las normas especificadas para las frecuencias de satélites"* (Asamblea Legislativa de la República de Costa Rica, 2008).

h) Adopta una serie de principios y objetivos de servicio universal, acceso universal y solidaridad, así como los mecanismos de financiamiento para el logro de esos objetivos.

i) Dedica un capítulo completo al tema de la protección de la privacidad y los derechos de los usuarios finales, a lo largo del cual establece que cualquier contrato de servicios de telecomunicaciones firmado en el país, deberá tener en cuenta tanto la privacidad como los derechos e intereses de los usuarios finales.

   Se debe resaltar que a lo largo de este punto la Ley asigna una serie de responsabilidades en materia de protección de datos personales, que se tornan valiosas para la presente investigación; dentro de ellas están las siguientes:

   - Corresponde a la SUTEL la atención a reclamaciones de violación a los derechos del usuario.
   - Corresponde a los operadores y proveedores de servicios garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de datos personales de sus abonados y usuarios finales, para lo cual deben adoptar medidas técnicas y administrativas idóneas adicionales a las fijadas reglamentariamente. Asimismo, deberán garantizar que las comunicaciones y datos de tráfico por ellos almacenados no sean *"escuchadas, gravadas, almacenadas, intervenidas ni vigiladas por terceros sin su consentimiento, salvo cuando se cuente con la*

*autorización judicial correspondiente"* (Asamblea Legislativa de la República de Costa Rica, 2008).

- Corresponde a los operadores y proveedores el eliminar o anonimizar los datos de tráfico y localización cuando no sean necesarios para la transmisión de una comunicación o la prestación de un servicio; estos son tratables solamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago[267].

j) Dicta las disposiciones relevantes en materia del régimen de competencia aplicable a las empresas de telecomunicaciones en nuestro país, el régimen de acceso e interconexión y los cánones de telecomunicaciones vigentes.

k) Establece el régimen sancionatorio aplicable en nuestro país. Determina en este punto como *infracciones muy graves*[268] tanto *utilizar la información de los usuarios finales para fines no autorizados en la ley* como *violar la privacidad o intimidad de los usuarios finales*.

l) Establece los criterios de prescripción de la responsabilidad administrativa, determinando que *"La acción para reclamar responsabilidad administrativa prescribirá en el plazo de cuatro años ([269]), contado a partir del momento en el que se*

[267] A pesar de que la ley establece de manera clara estas disposiciones en su artículo 43, en entrevista con Maryleana Méndez, directora de la junta directiva de la SUTEL, se logró determinar que en la actualidad los operadores y proveedores de servicio no cumplen con estas disposiciones en tanto determinar claramente en qué momento puede "expirar el plazo durante el cual puedan impugnarse legalmente las facturas o exigirse el pago" en nuestro país es sumamente difícil dado el conocido rezago de nuestro sistema judicial.
Esta situación ha llevado a los operadores y proveedores a almacenar esta información por largos periodos de tiempo (sin llegar por supuesto a anonimizar dichos datos dada la relevancia potencial de los mismos) y a pesar de lo anterior la Superintendencia no ha logrado corregir la situación pues se encuentran ante una "zona gris" (Méndez, Marín, & Steller, 2013).

[268] Sancionables mediante una multa de entre cero coma cinco por ciento (0,5%) y hasta un uno por ciento (1%) de los ingresos brutos del operador o proveedor obtenidos durante el período fiscal anterior

[269] Debemos llamar la atención sobre el plazo establecido en el inciso a del artículo 71 de la ley pues nos permite determinar la situación real del almacenamiento de los datos personales en nuestro país. Tal

*cometió la infracción. No obstante, en los casos de infracciones continuadas o de efectos permanentes, el plazo se computará desde el día que se cometió la última infracción o desde que cesó la situación ilícita, respectivamente"* (Asamblea Legislativa de la República de Costa Rica, 2008).

### *Reglamento a la Ley General de Telecomunicaciones*

Dictado el 22 de septiembre de 2008 como Decreto Ejecutivo Nº 34765-MINAET, el Reglamento a la Ley General de Telecomunicaciones constituye un importante punto de inicio en la regulación específica y técnica del sector telecomunicaciones (Presidencia de la República de Costa Rica, 2008).

Específicamente este reglamento procura cumplir con los objetivos establecidos por la Ley General de Telecomunicaciones mediante la incorporación en el marco legal vigente, de un número de medidas dirigidas a regular con mayor detalle temas como: el espectro radioeléctrico; los títulos habilitantes (concesiones, autorizaciones y permisos); las disposiciones generales para los títulos habilitantes (derechos y obligaciones de los operadores, uso, diseño e inspección de redes públicas de

como mencionamos en la nota al pie de página Nº 217, los operadores han optado por almacenar la información hasta el momento en que esta deja de ser relevante en caso de que les sea imputada alguna conducta reprochable.
A partir de este razonamiento y de la información recopilada de fuentes oficiales en nuestro país los operadores se han dado el lujo de almacenar la información por los cuatro años necesarios para salvar su responsabilidad o asegurar su derecho de defensa en caso de ser imputados con algún tipo de responsabilidad administrativa.
Ante esta perspectiva, no podemos hacer más que preguntarnos si realmente serán eliminados o anonimizados dichos datos una vez cumplido ese plazo o si los operadores se valdrán de la tesis de que ante la posibilidad de ser imputados con una infracción continuada estos deben salvaguardar una copia sin anonimizar de dichos datos de manera indefinida.
Claramente esta es una cuestión que debe ser examinada con detenimiento tanto por SUTEL como por la Agencia de Protección de Datos de los Habitantes de nuestro país.

telecomunicaciones); servicios de radiodifusión y televisión (incluyendo reglamentación sobre los locutores y los servicios de audio y televisión por subscripción); el Registro Nacional de Telecomunicaciones y las audiencias públicas.

Tal como se estableció con anterioridad, este reglamento toma importancia al aclarar los procedimientos por seguir en cada caso[270] y generar una conexión clara con los diversos planes técnicos fundamentales que deben ser seguidos por los diversos interesados al prestar sus servicios al público.

### *Ley Nº 7566 "Ley de Creación del Sistema de Emergencias 911"*

Dictada el 18 de diciembre de 1995, y posteriormente reformada en parte por la Ley Nº 8642, la Ley Nº 7566, crea el sistema de emergencias 911 y establece una serie de disposiciones tendientes a asegurar el buen funcionamiento de este.

Esta ley resulta relevante al tema en cuestión, en tanto la Ley General de Telecomunicaciones modifica su artículo 10 y establece como responsabilidad exclusiva de los proveedores de servicios de telefonía el *"diseñar, adquirir, instalar, mantener, reponer y operar, técnica y administrativamente, un sistema de telecomunicaciones ágil, moderno y de alta calidad tecnológica, que permita atender y transferir las llamadas, según los requerimientos de los usuarios del Sistema. Los proveedores de servicios de telefonía, públicos o privados, que operen en el país deberán poner a disposición los recursos de infraestructura que el Sistema de Emergencias 9-1-1 requiera para el cumplimiento eficiente y*

[270] Como por ejemplo los procedimientos por seguir durante las audiencias públicas que debe convocar y dirigir la SUTEL antes de aprobar estándares o reglamentos técnicos.

*oportuno de sus servicios, en aspectos que garanticen que las llamadas realizadas por la población deberán ser recibidas por los centros de atención que el Sistema habilite y* ***se brindarán los datos de localización del usuario que disponga el acceso al servicio****" [El subrayado no es del original]* (Asamblea Legislativa de la República de Costa Rica, 1995).

Esta modificación al artículo 10 tiene grandes implicaciones para los sistemas de telecomunicaciones convergentes implementados en nuestro país. Desde un punto de vista técnico, la puesta en disposición de los recursos de infraestructura a favor del sistema 911 deberá ser implementada de forma diferente en una red VoIP que en una red telefónica tradicional. Asimismo, salta a la vista que la ley exige a los proveedores liberar la información de localización del usuario para cada llamada realizada a este sistema[271].

### *Ley Nº 7593 "Ley de la Autoridad Reguladora de Servicios Públicos"*

Aprobada el 9 de agosto de 1996, esta ley crea y regula la Autoridad Reguladora de Servicios Públicos (Asamblea Legislativa de la República de Costa Rica, 1996). Tal como se estableció con anterioridad, esta ley se torna relevante para el sector telecomunicaciones en tanto determina las facultades de la Junta de Directores de ARESEP con respecto a SUTEL, e incluye las disposiciones que legitiman a este ente

[271] A pesar de esta situación, a raíz de una serie de entrevistas realizadas con doña Maryleana Méndez (directora de la junta directiva de SUTEL), y don Adrián Marín (ingeniero de la dirección general de calidad de SUTEL) se logró determinar que en la actualidad las dificultades técnicas han logrado ser subsanadas, en especial gracias al proceso que culminó mediante la adopción de la resolución RCS-251-2012 por parte de la SUTEL (Superintendencia de Telecomunicaciones, 2012).
Asimismo, la entrega de datos personales debe ser entendida en el marco de confidencialidad propio de este sistema (ver Dictamen C-233-2002 de la Procuraduría General de la República) (Méndez, Marín, & Steller, 2013)

descentralizado a generar los planes técnicos fundamentales que fueron necesarios para poner en marcha el sector luego de su liberalización.

## *Marco Regulatorio Vigente en Materia de Protección de Datos Personales*

Una vez examinado el contexto legal que rodea en nuestro país al sector telecomunicaciones, es necesario comprender los esfuerzos realizados hasta la fecha por nuestro país en materia de protección de datos internacionales, tanto en el plano nacional como internacional.

### Normativa Internacional Vigente para la República de Costa Rica en Materia de Protección de Datos Personales

Desde el plano internacional, Costa Rica puede ser caracterizada por ser parte de varios convenios dirigidos (o que incluyen cláusulas referentes) a la protección de datos personales que poseen diversos grados de vinculación para nuestro país. A continuación se procederá a examinarlos individualmente, procurando determinar específicamente sus implicaciones en el tema de interés.

#### *Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional*

Adoptada por la Asamblea General de las Naciones Unidas el 15 de noviembre de 2000 y ratificada por Costa Rica mediante decreto ejecutivo Nº 31270 del 01 de julio de 2003 (Asamblea Legislativa de la República de Costa Rica, 2000), la Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional (conocida también como Convención de Palermo) busca promover la cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional.

Para ello, la convención establece una serie de disposiciones referentes a la penalización y combate de la delincuencia organizada, a la vez que contempla una serie de disposiciones relevantes para el tratamiento de la información que deberán realizar los Estados firmantes. Específicamente, esta convención dispone lo siguiente:

1) Cada Estado parte garantizará que sus respectivas autoridades relevantes sean capaces de cooperar e intercambiar información en el nivel nacional y el internacional.
2) Creará cada Estado dependencias de inteligencia financiera encargadas de la recopilación, análisis y difusión de información sobre posibles actividades de blanqueo de dinero.
3) Responder a solicitudes internacionales de cooperación con miras al decomiso del producto del delito, los bienes, el equipo u otros instrumentos relacionados con el crimen organizado.
4) Prestar la más amplia asistencia judicial recíproca respecto de investigaciones, procesos y actuaciones judiciales relacionadas con los delitos contemplados por la Convención. Para ello, las autoridades judiciales pueden transmitir información relativa a cuestiones penales a una autoridad competente de otro

Estado parte, sin solicitud previa (sin menoscabo del Derecho interno y debiendo responder el Estado receptor a solicitudes de confidencialidad de la información).

5) Transmitir ante solicitud de asistencia judicial (y conforme las condiciones que juzgue apropiadas) una copia total o parcial de los documentos oficiales o de documentos o datos que obren en su poder y que, conforme a su Derecho interno, no estén al alcance del público en general.
6) No transmitir ni utilizar sin previo consentimiento del Estado parte requerido, la información o las pruebas proporcionadas por el Estado parte requerido para investigaciones, procesos o actuaciones judiciales distintos de los indicados en la solicitud.
7) Establecer procedimientos para la protección de los testigos, incluyendo la prohibición total o parcial de revelar información relativa a su identidad y paradero.

Finalmente, es necesario recordar que la Convención de Palermo *"sólo es aplicable en los denominados "delitos graves", es decir, aquellos en que la pena por la comisión de un delito tiene como retribución o castigo una máxima de al menos 4 años de prisión o más.* (Organización de los Estados Americanos, 2011)*;* esta situación generaba un problema al contrastarse con las antiguas disposiciones de nuestro Código Penal que castigaba estos delitos con penas de prisión de seis meses a dos años, lo cual hacia inaplicables las disposiciones de esta convención en los casos de delitos informáticos producidos en nuestro país.

Afortunadamente, esta situación fue subsanada mediante la promulgación en julio del 2012 de la Ley Nº 9048, la cual aumentó la pena de prisión contemplada por el artículo 196 bis de nuestro Código Penal de tres a seis años y de cuatro a ocho años en caso de cumplirse dos condiciones específicas que se analizarán más adelante.

### *Convención Interamericana sobre Extradición*

Ratificada por Costa Rica mediante la Ley Nº 7953 de 21 de diciembre de 1999, la Convención Interamericana sobre Extradición se dirige a generar la obligación entre los Estados partes, de extraditar ante solicitud de otro Estado parte *"a las personas requeridas judicialmente para procesarlas, así como a las procesadas, las declaradas culpables o las condenadas a cumplir una pena de privación de libertad" (Organización de los Estados Americanos, 2011).*

Con tal de cumplir esta obligación, establece la Convención la necesidad de adjuntar, junto con la solicitud de extradición *"los datos personales que permitan la identificación del reclamado, indicación sobre su nacionalidad e, incluso, cuando sea posible, su ubicación dentro del territorio del Estado requerido, fotografías, impresiones digitales o cualquier otro medio satisfactorio de identificación" (Organización de los Estados Americanos, 1981).*

### *Declaración de La Antigua sobre Datos Personales*

Adscrita por Costa Rica al momento de su creación durante el II Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua, Guatemala en 2003, y cuenta también con la anuencia de representantes de los países de Argentina, Brasil, Chile, El Salvador, España, Guatemala, Nicaragua, Perú, Portugal, Uruguay y México

Caracterizada por comprender a la protección de datos personales *"...como un auténtico derecho fundamental de las personas, sobre todo en orden al respeto a su intimidad y de su facultad de control y disposición sobre los mismos." (Representantes de los países iberoamericanos, 2003)*, esta Declaración dio lugar a dos hechos de gran relevancia en el nivel iberoamericano: la constitución de la Red Iberoamericana de Protección de Datos y el posterior reconocimiento del derecho fundamental a la protección de datos de carácter personal por parte de los Jefes de Estado y de Gobierno reunidos en Santa Cruz de la Sierra; la cual en su artículo 45 establece que:

*"45. Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad" (XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, 2003).*

A pesar de constituir un punto importante en la historia de la protección de datos personales de nuestro país, se debe reconocer, junto con los representantes de Costa Rica ante la OEA, que lastimosamente *"la Declaración de La Antigua no es un instrumento de derecho positivo ni ha sido formalmente aprobado como tal por la Asamblea Legislativa, por*

*lo cual sólo podría tenerse como una declaración de intenciones para el Estado, pero sin verdadero efecto coercitivo" (Organización de los Estados Americanos, 2011).*

### *Estatuto de Roma de la Corte Penal Internacional*

Suscrito por sus Estados miembros el 7 de octubre de 1998 y ratificado en Costa Rica por la Ley 8083 del 07 de febrero del 2001, el Estatuto de Roma de la Corte Penal Internacional no solamente crea esta importante institución internacional, sino que también adopta algunas disposiciones relevantes a la protección de datos personales.

Se pueden encontrar varios ejemplos de este tipo de disposiciones a lo largo del articulado del Estatuto; por ejemplo el otorgar a sus fiscales la potestad para *"adoptar o pedir que se adopten las medidas necesarias para asegurar el carácter confidencial de la información, la protección de una persona o la preservación de las pruebas"* (Organización de las Naciones Unidas, 1998, pág. 30) mediante el inciso f de su artículo 54; o asignar a la Sala de Cuestiones Preliminares la función *de "asegurar la protección y el respeto de la intimidad de víctimas y testigos, la preservación de pruebas, la protección de personas detenidas o que hayan comparecido en virtud de una comparecencia, así como la protección de información que afecte a la seguridad nacional"* (Organización de las Naciones Unidas, 1998, pág. 32)a lo largo de su artículo 57.

### *Acuerdo de Cooperación Ambiental entre el Gobierno de Costa Rica y el Gobierno de Canadá*

Suscrito el 23 de abril de 2001 y aprobado mediante Ley Nº 8286 de 17 de junio de 2002; el Acuerdo de Cooperación Ambiental con el Gobierno de Canadá se constituye como parte del marco legal que da soporte a la participación Internacional de Costa Rica en los procesos de protección de datos personales, al incluir elementos referentes a la privacidad en un documento de índole ambiental.

Se encontrarán tales precisiones a lo largo del artículo 16 del Acuerdo, el cual reza lo siguiente:

*"ARTÍCULO 16 - Protección de información*

*Las partes otorgarán cualquier información solicitada de conformidad con este acuerdo, a menos que la divulgación de esa información estuviera prohibida o exenta de divulgación bajo sus respectivas leyes y reglamentos, incluyendo aquellas concernientes al acceso de información y privacidad"* (Asamblea Legislativa de la República de Costa Rica, 2003).

Con respecto a este Acuerdo, debe concordarse con los representantes de nuestro país ante la OEA al afirmar que: *"Si bien no se trata propiamente de un acuerdo de cooperación en materia de protección de datos, es muestra de la obligación de Costa Rica de dar información dentro del inicio o transcurso de una investigación transnacional" (Organización de los Estados Americanos, 2011).*

### *Acuerdo entre el Gobierno de la República de Costa Rica y el Gobierno de la República Francesa, Relativo a la Readmisión de Personas en Situación Irregular*

Firmado en la ciudad de San José, Costa Rica el 16 de junio de 1998 y aprobado como Ley Nº 7993 el 7 de marzo de 2000, el Acuerdo entre el Gobierno de la República de Costa Rica y el Gobierno de la República Francesa, relativo a la readmisión de personas en situación irregular, incluye un número importante de disposiciones dirigidas a fortalecer la lucha contra la inmigración irregular.

Dentro de su articulado, el Acuerdo menciona expresamente la protección de datos personales al establecer que:

*"Los datos personales necesarios para la ejecución del presente Acuerdo y comunicados por las Partes contratantes, deben ser tratados y protegidos según las legislaciones relativas a la protección de datos en vigencia en cada Estado.*

*En este marco:*

*1°- La Parte contratante requerida utiliza los datos comunicados exclusivamente para los fines previstos por el presente Acuerdo.*

*2°- Cada una de las Partes contratantes informa a la otra Parte contratante, por solicitud de esta, sobre la utilización de los datos comunicados.*

*3°- Los datos comunicados solo pueden ser tratados por las autoridades competentes de la ejecución del presente Acuerdo. Los datos solo pueden ser transmitidos a otras personas si se cuenta con la previa autorización escrita de la Parte contratante que las había comunicado"* (Gobiernos de las Repúblicas de Costa Rica y Francia, 1998, pág. 5).

### *Acuerdo de Diálogo Político y Cooperación entre la Comunidad Europea y sus Estados Miembros y las Repúblicas de Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá*

Firmado el 15 de diciembre de 2003 y ratificado por Costa Rica como Ley No. 8919 de 16 de diciembre de 2010, el Acuerdo de Diálogo Político y Cooperación procura reforzar y ampliar la cooperación prevista en el Acuerdo Marco de Cooperación de 1993 y se enfoca en tres objetivos fundamentales, a saber:

a) *"Fomento de la estabilidad política y social a través de la democracia, el respeto de los derechos humanos y la buena gobernanza;*
b) *Profundización del proceso de integración regional entre los países centroamericanos (…)*
c) *Reducción de la pobreza y fomento de un acceso más equitativo a los servicios sociales y a los frutos del crecimiento económico (…)" (Comunidad Europea y Gobiernos Centroamericanos, 2003, pág. 11).*

Con miras a cumplir tales objetivos el Acuerdo incluye dentro de su articulado un conjunto amplio de ámbitos de cooperación entre las partes. Específicamente relevantes para los objetivos del presente trabajo resultan los artículos 35 y 58, los cuales se refieren a la cooperación en materia de protección de datos y a la protección de datos respectivamente.

El artículo 35 establece que:

*"Cooperación en materia de protección de datos*

1. *Las Partes acuerdan cooperar para garantizar la protección de los datos personales y de otro tipo en su tratamiento, con vistas a promover las normas internacionales más estrictas.*
2. *Las Partes acuerdan también cooperar para mejorar el nivel de protección de los datos personales y trabajar en aras de su libre circulación entre las Partes, teniendo en cuenta debidamente las respectivas legislaciones internas" (Comunidad Europea y Gobiernos Centroamericanos, 2003, pág. 32).*

Por su parte, el artículo 58 del Acuerdo especifica:

*"Protección de los datos*

*A los efectos del presente Acuerdo, las Partes acuerdan dar un elevado nivel de protección al tratamiento de datos personales y de otra índole, compatible con las más estrictas normas internacionales".*

Con base en estos dos artículos se puede establecer entonces que nuestro país se ha comprometido a establecer fuertes relaciones de cooperación con la Comunidad Europea, con miras a garantizar tanto la libre circulación de la información entre los Estados parte como el más estricto nivel de protección de datos personales.

### *Acuerdo y Protocolo para el Intercambio de Información en Materia Tributaria con el Reino de los Países Bajos.*

Firmados en San José, Costa Rica el 29 de marzo de 2011 y aprobado por la Asamblea Legislativa como Ley Nº 9040 el 03 de mayo de 2012, el Acuerdo y el Protocolo para el

intercambio de información en materia tributaria, procuran facilitar el intercambio de información de interés para la administración y aplicación del Derecho interno de las partes en materia de impuestos.

Para lograr tal fin, se dispone en su articulado una serie de acuerdos con respecto al accionar requerido de ambas partes, frente a un requerimiento de la contraparte respectiva de facilitar[272] dicha información relevante. Específicamente, el artículo 5 del Acuerdo permite a las partes requerir y obtener los siguientes tipos de información:

a) *"información que obre en poder de bancos, otras instituciones financieras y cualquier persona que actúe en calidad representativa o fiduciaria, incluyendo designados y fiduciarios;*
b) *información relativa a la propiedad de sociedades, sociedades de personas, fideicomisos, fundaciones, "Anstalten" y otras personas, incluyendo, dentro de los constreñimientos del artículo 2, información sobre propiedad respecto de todas las personas que componen una cadena de propiedad; en el caso de fideicomisos, información sobre los fideicomitentes, fiduciarios y beneficiarios; y en el caso de fundaciones, información sobre los fundadores, los miembros del consejo de la fundación, y los beneficiarios. Aún más, este Acuerdo no impone una obligación a las Partes contratantes de obtener o proporcionar información sobre la propiedad en relación con sociedades cotizadas en Bolsa o fondos o planes de inversión colectiva públicos, a menos que dicha información pueda ser obtenida sin que ocasione dificultades desproporcionadas"* (Asamblea Legislativa de la República de Costa Rica, 2012, pág. 4).

[272] E incluso de obtenerla utilizando todas las medidas relevantes en caso de no contar con ella la parte requerida.

Tomando en consideración la amplitud potencial de la información que puede ser solicitada por la contraparte respectiva y los potenciales roces con la protección de los datos personales, el protocolo del Acuerdo establece en su artículo 1 una serie de disposiciones concernientes a la protección de datos, según las cuales:

*"Si han sido intercambiados datos personales bajo el Acuerdo entre el Reino de los Países Bajos y la República de Costa Rica para el intercambio de información en materia tributaria (en adelante referido como "el Acuerdo"), se aplicarán las siguientes disposiciones adicionales:*

a) *la autoridad receptora podrá usar dichos datos únicamente para el propósito señalado y estará sujeta a las condiciones prescritas por la autoridad suministradora; dicho uso también estará permitido, sujeto a la autorización escrita requerida bajo el artículo 8, para la prevención y enjuiciamiento de delitos graves y con el propósito de enfrentar amenazas graves a la seguridad pública;*
b) *la autoridad receptora deberá informar a la autoridad suministradora, si así se lo solicita, sobre el uso de los datos suministrados;*
c) *los datos personales deberán suministrarse únicamente a las agencias responsables. Cualquier suministro subsecuente de la información a otras agencias podrá efectuarse únicamente con la aprobación por escrito previa de la autoridad suministradora;*
d) *la autoridad suministradora estará obligada a tener todo cuidado razonable para asegurarse que los datos a suministrar sean precisos y que sean necesarios y proporcionados para los propósitos para los cuáles hayan sido suministrados. Deberá observarse cualquier prohibición de suministro de datos prescrita en virtud del Derecho interno aplicable. Si resultara que se han suministrado datos no precisos o datos que no debieron haber sido suministrados, la autoridad receptora deberá ser informada de esto sin dilación. Esa autoridad estará obligada a corregir o borrar esos datos sin dilación;*

e) *si así lo solicita, la persona interesada deberá ser informada de los datos suministrados en relación con ella, o del uso para el cuál dichos datos servirán. No será obligatorio proveer esta información si una vez sopesados todos los factores, se considera que el interés público de negar esa información es superior al de la persona interesada en recibirla. En todos los demás casos, el derecho de la persona interesada de ser informada de los datos existentes relacionados con ella deberá regirse por la ley nacional de la Parte contratante en cuyo territorio soberano se haya hecho la solicitud de información;*

f) *la autoridad receptora deberá soportar responsabilidad de conformidad con su Derecho interno en relación con cualquier persona que sufra daño ilegal como resultado de los datos suministrados conforme a este Protocolo. En relación con la persona que sufra daño ilegal, la autoridad receptora no podrá declarar en su defensa que el daño ha sido causado por la autoridad suministradora;*

g) *si el Derecho interno de la autoridad suministradora dispone, en relación con los datos personales suministrados, que en cierto período de tiempo deberán borrarse, dicha autoridad deberá informarlo adecuadamente a la autoridad receptora. Independientemente de dichos períodos, los datos personales suministrados deberán ser borrados una vez que dejen de ser requeridos para el propósito para el cual fueron suministrados;*

h) *las autoridades que suministren y que reciban estarán obligadas a mantener registros oficiales del suministro y recibo de datos personales;*

i) *las autoridades que suministren y que reciban estarán obligadas a tomar medidas efectivas para proteger los datos personales suministrados contra acceso no autorizado, alteración no autorizada y comunicación no autorizada"* (Asamblea Legislativa de la República de Costa Rica, 2012, pág. 9).

Evidentemente los contenidos tanto del Acuerdo como del Protocolo poseen en la actualidad aplicabilidad vinculante únicamente con respecto a los datos tributarios ya mencionados. Asimismo, sobra recordar que de conformidad con su carácter bilateral el Acuerdo no puede ser dar pie para que el gobierno de nuestro país facilite dicha información u ordene la aplicación de los protocolos de seguridad de la información y de protección de datos establecidos a lo largo de este documento, para aquellos datos no relacionados con los requerimientos realizados por parte del gobierno Holandés.

A pesar de estas disposiciones, tal como se podrá analizar más adelante, varias de las disposiciones plasmadas tanto en el Acuerdo como en el Protocolo han sido reiteradas en el nivel nacional por nuestra Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.

### *Convención Internacional para la Protección de todas las Personas contra las Desapariciones Forzadas*

Firmada el 20 de diciembre de 2006 y ratificada por Costa Rica el 16 de febrero de 2012, esta convención procura evitar las desapariciones forzadas[273] mediante la puesta en común de una serie de disposiciones dirigidas a la tipificación común de dicho fenómeno como un crimen de lesa humanidad.

[273] Definida por el artículo 2 de la convención como "El arresto, detención, secuestro o cualquier otra forma de privación de libertad por agentes del Estado o por personas o grupos de personas que actúan con su autorización, apoyo o la aquiescencia del Estado, seguida de la negativa a reconocer dicha privación de la libertad o del ocultamiento de la suerte o el paradero de la persona desaparecida, sustrayéndola a la protección de la ley." (Organización de las Naciones Unidas, 2006).

Se puede afirmar que esta convención internacional se relaciona con el tema de la presente investigación, en tanto su artículo 20 se dedica a establecer disposiciones relevantes al acceso a la información, y específicamente establece lo siguiente:

*"Artículo 20*

*1 Únicamente en el caso en que una persona esté bajo protección de la ley y la privación de libertad se halle bajo control judicial, el derecho a las informaciones previstas en el artículo 18 podrá limitarse, sólo a título excepcional, cuando sea estrictamente necesario en virtud de restricciones previstas por la ley, y si la transmisión de información perjudicase la intimidad o la seguridad de la persona o el curso de una investigación criminal, o por otros motivos equivalentes previstos por la ley, y de conformidad con el derecho internacional aplicable y con los objetivos de la presente Convención. En ningún caso se admitirán limitaciones al derecho a las informaciones previstas en el artículo 18 que puedan constituir conductas definidas en el artículo 2 o violaciones del párrafo 1 del artículo 17"* (Organización de las Naciones Unidas, 2006).

Tomando en consideración el texto del articulado y el estudio ya realizado del Derecho comparado relevante en materia de protección de datos personales, es posible entender que las referencias hechas por el artículo 20 de la Convención se relaciona tanto con el derecho a la información como con el habeas data latinoamericano[274], por lo que resulta fundamental recalcar la excepcionalidad de las limitaciones a la que se refiere la Convención.

[274] Recordemos que en el caso de varios países sudamericanos, el habeas data es constituido como derecho fundamental en tanto se busca responder al clamor ciudadano por el acceso a información sobre los múltiples casos de desapariciones forzadas que se dieron a lo largo de la historia.

### *100 Reglas de Brasilia sobre Acceso a la Justicia de las Personas en Condición de Vulnerabilidad*

Fueron elaboradas por un grupo de trabajo constituido en el seno de la Cumbre Judicial Iberoamericana y aprobadas el 6 de marzo de 2008 por la XIV Cumbre Judicial Iberoamericana en Brasilia. Se crearon como un conjunto de cien estándares básicos para ser seguidos por las más importantes redes del sistema judicial iberoamericano; estas reglas poseen un gran valor declarativo, a pesar de lo cual aún no han sido ratificadas oficialmente por la Asamblea Legislativa de nuestro país.

A pesar de esta situación, la importancia de las cien reglas de Brasilia para el contexto judicial costarricense no puede ser menospreciada. En palabras de los representantes de Costa Rica ante la OEA, si bien es cierto que las Reglas de Brasilia *"no han sido aprobadas formalmente por la Asamblea Legislativa, bien podrían invocarse como quebrantadas pues nuestra jurisprudencia constitucional ha establecido que cualquier norma internacional que tenga carácter protector de derechos humanos puede ser invocada en caso de quebranto, aunque la ratificación positiva no se haya dado" (Organización de los Estados Americanos, 2011)*.

La sección cuarta de las reglas se refiere a la protección de la intimidad, para lo cual establece tres estándares mínimos relacionados con este tema, a saber:

*"1.- Reserva de las actuaciones judiciales*

> *(80) Cuando el respeto de los derechos de la persona en condición de vulnerabilidad lo aconseje, podrá plantearse la posibilidad de que las actuaciones jurisdiccionales orales*

*y escritas no sean públicas, de tal manera que solamente puedan acceder a su contenido las personas involucradas.*

*2.- Imagen*

*(81) Puede resultar conveniente la prohibición de la toma y difusión de imágenes, ya sea en fotografía o en vídeo, en aquellos supuestos en los que pueda afectar de forma grave a la dignidad, a la situación emocional o a la seguridad dela persona en condición de vulnerabilidad.*

*(82) En todo caso, no debe estar permitida la toma y difusión de imágenes en relación con los niños, niñas y adolescentes, por cuanto afecta de forma decisiva a su desarrollo como persona.*

*3.- Protección de datos personales*

*(83) En las situaciones de especial vulnerabilidad, se velará para evitar toda publicidad no deseada de los datos de carácter personal de los sujetos en condición de vulnerabilidad.*

*(84) Se prestará una especial atención en aquellos supuestos en los cuales los datos se encuentran en soporte digital o en otros soportes que permitan su tratamiento automatizado"* (XIV Cumbre Judicial Iberoamericana, 2008).

### *Reglas de Heredia sobre Difusión de Información Judicial*

Aprobadas durante el Seminario Internet y Sistema Judicial realizado en la ciudad de Heredia, Costa Rica, los días 8 y 9 de julio de 2003 con la participación de poderes

judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay; las Reglas de Heredia sobre Difusión de Información Judicial en Internet constituyen un conjunto de estándares voluntarios asumidos por las diversas organizaciones allí representadas en relación con sus proyectos de acceso a la información por medio de internet.

En su forma final, las Reglas de Heredia comprenden un conjunto de diez reglas, cuatro definiciones y cinco alcances que se refieren a los siguientes puntos:

> Regla 1: Define la finalidad de la difusión en internet de las sentencias y resoluciones judiciales como *"a) el conocimiento de la información jurisprudencial y la garantía de igualdad ante la ley; b) para procurar alcanzar la transparencia de la administración de la justicia" (Seminario Internet y Sistema Judicial, 2003).*
>
> Regla 2: Procura asegurar el inmediato acceso de las partes o quienes tengan interés legítimo en la causa, a sus movimientos, citaciones o notificaciones.
>
> Regla 3: Reconoce el derecho de oposición del interesado, a que los datos que le conciernan sean objeto de difusión.
>
> Regla 4: Busca asegurar la adecuación al fin de los motores de búsqueda[275] al alcance y finalidades con que se difunde la información judicial.

[275] Comprendidos como "las funciones de búsqueda incluidas en los sitios en Internet de los Poderes Judiciales que facilitan la ubicación y recuperación de todos los documento en la base de datos, que satisfacen las características lógicas definidas por el usuario, que pueden consistir en la inclusión o exclusión de determinadas palabras o familia de palabras; fechas; y tamaño de archivos, y todas sus posibles combinaciones con conectores booleanos" *(Seminario Internet y Sistema Judicial, 2003).*

Regla 5: Establece que *"Prevalecen los derechos de privacidad e intimidad, cuando se traten datos personales([276]) que se refieran a niños, niñas, adolescentes (menores) o incapaces; o asuntos familiares; o que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos; así como el tratamiento de los datos relativos a la salud o a la sexualidad; o víctimas de violencia sexual o domestica; o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales.*

*En este caso se considera conveniente que los datos personales de las partes, coadyuvantes, adherentes, terceros y testigos intervinientes, sean suprimidos, anonimizados o inicializados, salvo que el interesado expresamente lo solicite y ello sea pertinente de acuerdo a la legislación" (Seminario Internet y Sistema Judicial, 2003).*

Regla 6: Dicta que en caso de que la persona concernida haya alcanzado voluntariamente[277] el carácter de pública y el proceso esté relacionado con las razones de su notoriedad, prevalecerá las transparencia y el derecho de acceso a la información pública (excepto en cuestiones de familia o cuando exista

[276] Definidos por las Reglas como "Los datos concernientes a una persona física o moral, identificada o identificable, capaz de revelar información acerca de su personalidad, de sus relaciones afectivas, su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio físico y electrónico, número nacional de identificación de personas, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad o su autodeterminación informativa. Esta definición se interpretara en el contexto de la legislación local en la materia" *(Seminario Internet y Sistema Judicial, 2003).*

[277] Entendido esto por las reglas como referido "a funcionarios públicos (cargos electivos o jerárquicos) o particulares que se hayan involucrado voluntariamente en asuntos de interés público (en este caso se estima necesaria una manifestación clara de renuncia a una área determinada de su intimidad)" *(Seminario Internet y Sistema Judicial, 2003).*

protección legal específica), siendo necesario anonimizar[278] los datos de los terceros involucrados.

Regla 7: Tutela el equilibrio entre el derecho de acceso a la información y el derecho a la intimidad tanto en las bases de datos de sentencias como en las de información procesal, evitándose presentar en ellas criterios que no sea el número de identificación o el descriptor temático.

Regla 8: Sitúa bajo completo control de la autoridad pública el tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad.

Regla 9: Procura que los hechos mencionados por los jueces en sus sentencias se dirijan, en cuanto sea posible, únicamente a fundamentar su decisión, tratando de no invadir la esfera íntima de terceros, evitando incluso los detalles que puedan *"perjudicar a personas jurídicas o dar excesivos detalles sobre los moda operandi que puedan incentivar algunos delitos" (Seminario Internet y Sistema Judicial, 2003).*

Regla 10: Busca que las reglas anteriores sean respetadas también en la celebración de convenios con editoriales jurídicas.

Finalmente, las reglas declaran tanto su limitación al contexto del Internet como su carácter de reglas mínimas, abiertas al uso de procedimientos más rigurosos. Asimismo, reconocen que *"pretenden ser hoy la mejor alternativa o punto de partida para lograr un equilibrio entre transparencia, acceso a la información pública y derechos de*

[278] Definido por las Reglas como "todo tratamiento de datos personales que implique que la información que se obtenga no pueda asociarse a persona determinada o determinable" *(Seminario Internet y Sistema Judicial, 2003).*

*privacidad e intimidad. Su vigencia y autoridad en el futuro puede estar condicionada a nuevos desarrollos tecnológicos o a nuevos marcos regulatorios" (Seminario Internet y Sistema Judicial, 2003).*

### *Protocolo Facultativo de la Convención sobre los Derechos del Niño Relativo a la Venta de Niños, la Prostitución Infantil y Utilización de Niños en la Pornografía*

Aprobado mediante Ley No.8172 de 7 de diciembre de 2001, el Protocolo señala, entre otros temas, la obligación de los Estados de participar activamente en la protección de la intimidad e identidad de los menores y las menores víctimas a lo largo del proceso penal. Especialmente relevante para esto resultan las disposiciones de su artículo 8, el cual reza:

*"Artículo 8*

1. *Los Estados Partes adoptaran medidas adecuadas para proteger en todas las fases del proceso penal los derechos e intereses de los niños víctimas de las prácticas prohibidas por el presente Protocolo y, en particular, deberán:*

   *(…)*

   *e) Proteger debidamente la intimidad e identidad de los niños víctimas y adoptar medidas de conformidad con la legislación nacional para evitar la divulgación de información que pueda conducir a la identificación de esas víctimas"* (Organización de las Naciones Unidas, 2000).

## Normativa Nacional Relevante para la Protección de Datos Personales

Tal como se manifestó anteriormente en la introducción histórica al sector de telecomunicaciones, Costa Rica basa su sistema legal vigente en las disposiciones de su actual Constitución Política, la cual desde su creación incorporó un fuerte énfasis en el fortalecimiento de las garantías individuales y permitió la creación de un Estado de Derecho que cuenta con una larga historia de estabilidad política y democrática.

Como bien podrá el lector suponer, la Constitución Política de Costa Rica del 7 de noviembre de 1949 también representa un punto de referencia para la protección de datos personales, en tanto contempla muchos de los derechos fundamentales relacionados con ella.

De esta manera, el artículo 24 constitucional consagra los derechos a la intimidad, a la libertad y al secreto de las comunicaciones. Al afirmar que: *"Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier tipo de los habitantes de la república (…)",* este artículo protege muchas de las manifestaciones de la vida privada al establecer tanto la confidencialidad de la información privada[279],

[279] Supeditada únicamente al interés público que pueda surgir a partir de esa información, siendo el interés público el elemento fundamental a la hora de diferenciar los documentos públicos y los documentos privados.
Sobre este tema, vale la pena recalcar que según la Ley Nº 7425, serán considerados documentos privados "la correspondencia epistolar, por fax, télex, telemática o cualquier otro medio; los videos, los casetes, las cintas magnetofónicas, los discos, los disquetes, los escritos, los libros, los memoriales, los registros, los planos, los dibujos, los cuadros, las radiografías, las fotografías y cualquier otra forma de registrar información de carácter privado, utilizados con carácter representativo o declarativo, para ilustrar o comprobar algo" (Asamblea Legislativa de la República de Costa Rica, 1994).
Esta definición amplia sobre los documentos considerados privados debe verse extendida por el principio de equivalencia funcional plasmado en el artículo tercero de la ley Nº 8454, el cual establece que "Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos. En cualquier norma del ordenamiento jurídico en la

como los casos en los cuales esta confidencialidad puede ser violentada legítimamente mediante intervenciones.

En segundo lugar, reconoce nuestra Constitución Política la libertad de expresión al afirmar tanto que *"nadie puede ser inquietado ni perseguido por la manifestación de sus opiniones ni por acto alguno que no infrinja la ley"* (Asamblea Nacional Constituyente de la República de Costa Rica, 1949) como que *"Todos pueden comunicar sus pensamientos de palabra o por escrito, y publicarlos sin previa censura, pero serán responsables de los abusos que cometan en el ejercicio de este derecho, en los casos y del modo que la ley establezca"* (Asamblea Nacional Constituyente de la República de Costa Rica, 1949) en sus artículos 28 y 29 respectivamente.

En tercer lugar, este texto fundamental reconoce el derecho de acceso a la información al establecer sus artículos 27 y 30 respectivamente que *"Se garantiza la libertad de petición, en forma individual o colectiva, ante cualquier funcionario público o entidad oficial, y el derecho a obtener pronta resolución"* (Asamblea Nacional Constituyente de la República de Costa Rica, 1949) y que *"Se garantiza el acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público. Quedan a salvo los secretos de Estado"* (Asamblea Nacional Constituyente de la República de Costa Rica, 1949).

A pesar de hacer mención de los derechos supracitados, lastimosamente nuestra Constitución Política no contempla de manera expresa el derecho de autodeterminación informativa o las modalidades de protección de datos personales observadas en el derecho comparado (los procesos de habeas data y protección de

que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. (…)" (Asamblea Legislativa de la República de Costa Rica, 2005).

datos personales). Tal situación, aunada con la inexistencia (hasta hace pocos años) en nuestro país de legislación específicamente relacionada con el tema, tuvo como consecuencia la indefensión práctica del ciudadano al lidiar con afrentas a sus datos personales.

Frente a esta situación, la responsabilidad de subsanar tales falencias recayó en la Sala Constitucional de nuestro país. Esta situación implicó que la protección de datos personales fuera instituida inicialmente mediante la jurisprudencia constitucional[280], caracterizada por adoptar diversas posiciones respecto al tema a lo largo de su historia.

### *Tratamiento Histórico Jurisprudencial de la Protección de Datos Personales en Costa Rica*

Tal como se afirmaba en el punto anterior, los múltiples vacíos legales existentes en materia de protección de datos personales y la falta de un reconocimiento expreso del derecho de autodeterminación informativa en la Constitución Política de nuestro país, tuvo como consecuencia la indefensión del ciudadano frente a los abusos de las nuevas tecnologías de la información y la comunicación.

Ante tal situación, la jurisprudencia constitucional se tornó en el medio por lo cual los costarricenses pudieron detener dichas afrentas y defender sus derechos. Por medio de la interposición de recursos de amparo ante la Sala Constitucional (mejor conocida

[280] Debemos recordar que según el artículo 13 de la Ley de la Jurisdicción Constitucional, en nuestro país "los precedentes y la jurisprudencia de la jurisdicción constitucional son vinculantes erga omnes salvo para sí misma" (Asamblea Legislativa de la República de Costa Rica, 1989).

como Sala Cuarta), los individuos afectados en nuestro país por el tratamiento indiscriminado de sus datos personales lograron durante poco más de dos décadas paliar la inexistencia de entes judiciales y administrativos especializados en el país.

Evidentemente, el reto generado por esta ola de recursos de amparo relacionados con los nuevos derechos generados por la rápida evolución de las TICs en el país no fue fácilmente superado por nuestra Sala Constitucional. *"Precisamente por la confusión y desafío que representaba para los jueces la existencia reciente de un nuevo derecho como la autodeterminación informativa, apadrinado por corrientes de pensamiento igualmente novedosas que lo que lo apartaban de los conceptos tradicionales de la privacidad o intimidad, se estuvo emitiendo jurisprudencia confusa y contradictoria que en realidad no ayudaba a definir la defensa a favor de los ciudadanos" (Organización de los Estados Americanos, 2011, pág. 21)*[281].

De esta manera, la protección de datos personales y el derecho de autodeterminación informativa fueron estudiados por la Sala Constitucional en múltiples ocasiones, con lo cual se generaron miles de sentencias constitucionales que han demostrado una marcada tendencia evolutiva. Carvajal Pérez ha realizado un estudio extensivo de las tendencias históricas adoptadas por nuestra jurisprudencia constitucional en materia de protección de datos personales y con base en este actualmente reconoce la existencia de seis etapas (Carvajal Pérez, 2014), a saber:

[281] Y continúan recalcando los representantes de nuestro país ante la OEA que "aunado ello además a la presencia fuerte de empresas que procuraron desde siempre impedir que se legislara sobre el tema, pues ello afectaba sus intereses económicos. Por ello, era común encontrar sentencias constitucionales que avalaban las prácticas violatorias de dichas empresas, pues se partía del supuesto de que lo que interesaba proteger era solo la intimidad o la privacidad del demandante, pero no sus demás datos personales" (Organización de los Estados Americanos, 2011, pág. 21).

*Etapa de Reconocimiento Inconsciente*

Caracterizada esta primera etapa, según Carvajal Pérez, por verse reconocido este derecho por la Sala Constitucional *"sin saber que lo está reconociendo, defendiendo otros derechos fundamentales, como por ejemplo el principio de inocencia, la dignidad de la persona humana, entre otros. Principalmente en materia penal ordenando la desinscripción de determinados datos contenidos en fichas policiales, en registros de delitos cometidos, entre otros"* (Carvajal Pérez, 2013).

Según el autor (Carvajal Pérez, 2003), esta primera etapa puede verse reflejada en el contenido de resoluciones constitucionales como las siguientes:

Resolución Nº 2609-91

Relacionada con la fuga de información personal en el archivo criminal del Organismo de Investigación Judicial. Esta resolución afirma que "el carácter confidencial del Archivo no permite un acceso irrestricto a la información que contiene, ya que esa confidencialidad fue acordada para proteger la honra de las personas que se encuentran allí fichadas, de una posible afectación sin causa" (Sala Constitucional de la Corte Suprema de Justicia, 1991).

Resolución Nº 2680-94

La cual se torna relevante al establecer que: *"El derecho a la intimidad no se constituye en una potestad del sujeto de determinar la existencia o no de registros con informaciones de carácter personal ni la posibilidad de que con base en el derecho a la autodeterminación informativa éste pueda decidir qué aspectos deben o no ser registrados. La complejidad de las relaciones sociales y la necesidad de cumplimiento de las funciones del Estado exigen que se cuente con información indispensable para el cumplimiento de esos fines. En el*

*campo del control y combate de la criminalidad el Estado debe contar con los medios que le permitan realizar las investigaciones necesarias para individualizar a los responsables de las conductas delictivas y para alcanzar fines en la ejecución de las penas" (Sala Constitucional de la Corte Suprema de Justicia, 1994).*

*Etapa de Negación*

Comenzando a mediados de los años noventa, la *etapa de negación* se caracteriza, según Carvajal Pérez, porque la Sala Constitucional "comienza a rechazar los recursos de amparo presentados para la protección de la autodeterminación informativa, (para lo cual) establece diversos argumentos, (y) arguye diversas razones que llevan a entender que no se trata de materia propiamente protegible por la vía del amparo en la Sala Constitucional, que se trata de conflictos de otra naturaleza cuando la persona impugnada es un sujeto de derecho privado (Carvajal Pérez, 2013).

Esta etapa se encuentra plasmada en los análisis realizados a lo largo de resoluciones representativas (Carvajal Pérez, 2003); como por ejemplo:

Sentencia Nº 476-91

Que niega el Derecho al olvido en relación con el l Archivo Criminal del OIJ, al considerar que si bien es claro que el OIJ ha mantenido una reseña de las detenciones del interesado por más de diez años, *"lesiona los derechos fundamentales que le otorga nuestra Constitución Política y la Convención Americana sobre Derechos Humanos";* el hecho de que el imputado haya sido obligado a comparecer ante un tribunal legitima el accionar del OIJ para *"elaborar y*

*mantener su ficha y documentación respectiva en el Archivo Criminal creado con ese propósito" (Sala Constitucional de la Corte Suprema de Justicia, 1991).*

Sentencia Nº 2256-95[282]

Relacionada también con el Archivo Criminal del OIJ y que sustenta la conservación por plazos indefinidos de información personal (fotografía) como parte del registro criminal, en tanto considera que el OIJ se encuentra facultado por su ley orgánica para llevar a cabo un registro criminal que no viola, según la jurisprudencia, los derechos de los individuos registrados dado que posee "*efectos policiales, siendo de estricta confidencialidad, limitado su acceso a ciertas dependencias claramente definidas (Vid sentencias de esta Sala N.° 1490-90 y N.° 476-91)" (Sala Constitucional de la Corte Suprema de Justicia, 1995)*".

*Etapa de Reconocimiento Casuístico*

Afortunadamente la etapa de negación es corta en la jurisprudencia constitucional de nuestro país y es sucedida por una etapa que Carvajal Pérez llama de *reconocimiento casuístico* y que está caracterizada por el reconocimiento a la autodeterminación informativa *"no quizás desarrollando una doctrina consistente y amplia sino desarrollando casos concretos en materia crediticia, en materia comercial, en materia laboral y en materia*

[282] Relacionada también con el Archivo Criminal del OIJ y que sustenta la conservación por plazos indefinidos de información personal (fotografía) como parte del registro criminal en tanto considera que: "Lo cierto del caso es que el artículo 40 de la Ley Orgánica del Organismo de Investigación Judicial faculta a aquella dependencia para llevar un registro criminal de todas aquellas personas que fueran pasadas a las órdenes de autoridad judicial, lo cual en reiterada jurisprudencia no se le ha encontrado roces de constitucionalidad, pues lo que se pretende con el mismo es mantener un registro para efectos policiales, siendo de estricta confidencialidad, limitado su acceso a ciertas dependencias claramente definidas (Vid sentencias de esta Sala N.° 1490-90 y N.° 476-91)" (Sala Constitucional de la Corte Suprema de Justicia, 1995)

*penal que van generando los gérmenes de lo que será la regulación plena y que en una siguiente etapa produce una doctrina jurisprudencial genérica" (Carvajal Pérez, 2013).*

Según el autor supracitado, algunos de los elementos más representativos (Carvajal Pérez, 2003) de esta etapa pueden ser encontrados en las resoluciones siguientes:

Sentencia Nº 2805-98

La cual recuerda a las partes que los principios actuales del sistema judicial imponen al juez penal la función de ser controlador y garante de los derechos de los intervinientes en el proceso. Así, recuerda la sentencia que los *"representantes del Ministerio Público no tienen poderes decisorios, ni tienen capacidad para decretar, autónomamente, medidas que limiten, de alguna forma, derechos constitucionales fundamentales (libertad, intimidad, recepción de pruebas irreproductibles, etc.), reservándose esta materia a una autoridad judicial que será la que mantendrá un control sobre la investigación, protegiendo los derechos del acusado, sin comprometerse en la investigación del hecho denunciado" (Sala Constitucional de la Corte Suprema de Justicia, 1998).*

Sentencia Nº 8218-98

Dictada en respuesta a un recurso de inconstitucionalidad referido al Archivo Criminal del OIJ, esta sentencia hace especial referencia a los antecedentes penales de personas menores de edad retenidos de manera indefinida. Entre otras particularidades, reconoce esta sentencia por vez primera el derecho al olvido, a la vez que menciona la autodeterminación informativa al asegurar la prohibición de las penas perpetuas en el país (limitando con ello a un máximo de diez años el tiempo en que esta información puede ser retenida por el Centro de Información Policial).

*Asimismo, también resultan inconstitucionales las consecuencias a perpetuidad de los datos tenidos en los archivos policiales, en atención al principio de dignidad de la persona humana, valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión de respeto por parte de los demás. Estrechamente relacionado con el libre desarrollo de la personalidad y los derechos a la integridad física y moral, a la libertad de ideas y creencias, al honor, a la intimidad personal y familiar, y a la propia imagen; y que es universal, al no caber ninguna excepción ni discriminación, en tanto ha de permanecer inalterado, cualquiera que sea la situación en que la persona se encuentre (…). El principio de humanidad es el que dicta la inconstitucionalidad de cualquier pena o consecuencia del delito que cree un impedimento o consecuencia imborrable del delito, sea o no pena, debiendo cesar en algún momento. Por ello, la utilización del registro para dar información a los empleadores o para el cumplimiento de ciertos trámites administrativos (solicitudes de determinados permisos), constituye una violación de los derechos humanos, en tanto agrega una pena perpetua, que se extiende incluso a datos sobre procesos sufridos aún con resultado favorable. Por esta misma razón, es que los efectos a perpetuidad son contrarios a los principios constitucionales de razonabilidad y proporcionalidad, por los que únicamente son legítimas las restricciones a los derechos fundamentales que sean necesarias para conseguir el fin perseguido" (Sala Constitucional de la Corte Suprema de Justicia, 1998).*

*Etapa de Doctrina Jurisprudencial Genérica*

Etapa caracterizada por el reconocimiento efectivo por parte de la Sala Constitucional del derecho a la autodeterminación informativa. A lo largo de esta etapa, la Sala *"lo define, establece cuales son las reglas generales de actuación de los operadores de bases de datos, menciona, reconoce los derechos de la persona en relación al tratamiento de sus datos personales y solidifica muchos temas propios a la protección que la persona puede realizar ante las diversas instancias judiciales y administrativas para la protección de sus derechos (Carvajal Pérez, 2013).*

Como parte de esta labor, la Sala realiza a lo largo de este periodo un amplio desarrollo del habeas data y los principios atinentes al acopio, almacenamiento y empleo de las bases de datos. Asimismo, reconoció expresamente el derecho a la autodeterminación informativa y recogió sus postulados fundamentales (Carvajal Pérez, 2003).

Dentro de las sentencias más representativas de este periodo se pueden reconocer las siguientes:

> Voto Nº 4154-97
>
> Recurso de amparo relacionado con el derecho del trabajador de conocer los informes de investigación realizados por la Secretaría del Organismo de Investigación Judicial, a lo largo del cual: "La Sala estima que, en ejercicio del derecho de elección de su personal, el patrono puede recabar la información que sea necesaria para determinar si una persona es apta o no para el cargo al que aspira. En el proceso de selección debe ser riguroso, pues de lo contrario podría ser sujeto de responsabilidad objetiva -vgr. culpa in eligendo-. Sin embargo, en caso de que las personas soliciten acceso a la información que sobre ellas se haya recabado, ésta debe ser suministrada. Las pruebas anónimas, para el fin que sean, violan el derecho

fundamental a conocer lo que de la persona se dice o los datos que sobre ella se conservan, lo contrario es inadmisible en el sistema democrático y a la luz del Derecho de los Derechos Humanos" (Sala Constitucional de la Corte Suprema de Justicia, 1997).

Resolución Nº 5802-99

De especial relevancia para la presente investigación, esta resolución da respuesta a una acción de inconstitucionalidad interpuesta contra el artículo 40 de la Ley Orgánica del OIJ (la cual había fundamentado varias de las negativas anteriores al reconocimiento del derecho al olvido en el país), para lo cual estudia de manera innovadora el derecho a la intimidad y el derecho al habeas data y a continuación declara los contenidos de dichos derechos.

Para tal fin, no solo establece la resolución que *"el derecho a la intimidad tiene una conexión de sentido y función con otras garantías y derechos fundamentales (…) Para efectos de alcanzar una tutela de la persona realizable en el estado actual del desarrollo tecnológico, resulta indispensable considerar que los ciudadanos tienen derecho a conservar una facultad de control sobre el flujo de las informaciones personales que circulan en el entorno social*" (Sala Constitucional de la Corte Suprema de Justicia, 1999); también analiza como propios del habeas data el derecho al acceso; a la actualización; a la confidencialidad[283]; a la exclusión, a la

[283] Definido por la Sala como aquel derecho a través del cual "el sujeto exige que la información que él ha proporcionado o que ha sido legalmente requerida permanezca secreta para terceras personas, de forma tal que se controla el cumplimiento de los fines para los que la información es recolectada. En este caso la información recabada puede resultar correcta y haber sido adquirida por medios legítimos, pero se trata de información que no puede ser facilitada indiscriminadamente y tiende a que los datos no sean revelados salvo que obedezca a la solicitud de autoridad competente o del interesado" (Sala Constitucional de la Corte Suprema de Justicia, 1999).

inserción[284] y a saber del conocimiento de terceros sobre la información recolectada.

Finalmente, establece también la Sala mediante esta resolución, algunos lineamientos por seguir por parte del Estado con miras a asegurar su capacidad de llevar a cabo la persecución de las actividades delictivas. Específicamente menciona la sentencia la necesidad de asegurar la transparencia; la especificación de los fines del banco de datos; la creación de un órgano de control de la observancia de los preceptos legales en el tratamiento de datos personales[285]; las limitaciones a la recolección; la limitación del uso; la aplicación certera de los plazos de validez (olvido) de los datos; la obligación jurídica de confidencialidad; las exigencias relativas a la calidad de los datos; la información sobre la finalidad, uso y derechos de acceso y rectificación; el derecho de bloqueo; la justificación social del uso de los datos; y la limitación de los medios de recolección de los datos (Sala Constitucional de la Corte Suprema de Justicia, 1999).

Voto Nº 1345-98

Voto que resuelve un recurso de amparo contra sujetos de derecho privado ante una consulta de información crediticia de la recurrente en una base de datos que contenía datos incorrectos. Específicamente se determina que: *"El fin de este derecho consiste en que cualquier persona tenga la posibilidad de defenderse*

[284] Que según la Sala "se funda en las circunstancias en que los sujetos tienen un interés preciso en que sus propios datos sean insertados en un determinado banco de datos, los que fueron omitidos, junto a otros datos suyos que pueden modificar su perfil o despejar dudas al respecto" (Sala Constitucional de la Corte Suprema de Justicia, 1999).
[285] El cual no fue creado en el país sino hasta pasada más de una década de la emisión de la resolución en cuestión.

*contra calificaciones sospechosas incluidas en registros que sin darle derecho a rectificarlas o contradecirlas podrían llegar a causarle un grave perjuicio. (…) La Sala estima que la actuación de los recurridos al afectar las posibilidades de crédito de las amparadas, en virtud de un hecho pasado que tenía sus propios remedios, como la interposición oportuna del juicio ejecutivo, y de incluirla en un "libro negro" en razón de información errónea -crédito incobrable cuando en el mundo jurídico el mismo ha dejado de existir- lesiona el derecho a la intimidad de las amparadas"* (Sala Constitucional de la Corte Suprema de Justicia, 1998).

Voto Nº 754-02

A lo largo de este voto no solamente estudia la Sala los presupuestos de admisibilidad de un recurso de amparo interpuesto contra sujetos de derecho privado, sino que también presta gran atención a los principios de autodeterminación informativa que se ven involucrados en la administración de las bases de datos corporativas. Afirma la Sala al respecto que los datos personales que se encuentren en estas circunstancias deben cumplir fielmente con los principios de exactitud y precisión con miras a evitar producir perjuicios al interesado y a terceros *(Sala Constitucional de la Corte Suprema de Justicia, 2002)*.

*Etapa de Doctrina Jurisprudencial Específica*

La quinta etapa histórica de la jurisprudencia constitucional en esta materia se caracteriza, según Carvajal Pérez, porque la Sala comienza a analizar "*temas específicos, ya no resueltos casuísticamente, sino sobre la base de la doctrina jurisprudencial ya asentada*

*con anterioridad. Temas como el derecho al olvido, temas como la protección ante la manipulación de los datos de orden médico, entre otros, son los grandes temas que están en este momento ante la Sala Constitucional y que han llevado ante un desarrollo congruente con la doctrina genérica planteada pero que se diversifica y se* especializa" (Carvajal Pérez, 2013).

Dentro de las sentencias más representativas de esta etapa se encuentran:

Sentencia Nº 8996-02

Interpuesta contra la empresa Datum.net frente a la publicación de información personal por parte de la empresa ALUDEL (Sala Constitucional de la Corte Suprema de Justicia, 2002), esta sentencia realiza un análisis de las obligaciones del operador de una base de datos y *"reconoce los derechos a recibir información acerca del uso que será dado a los datos suministrados, al consentimiento necesario para que tales informaciones puedan ser recogidas, almacenadas y manipuladas, y sienta algunas bases de lo que deberá en el futuro ser la regulación de la transferencia nacional e internacional de datos entre diversos ficheros. Es decir, recoge muchos de los principios modernamente entendidos como propios de una adecuada protección de datos" (Carvajal Pérez, 2003).*

Sentencia Nº 2004-12239

En ella la Sala estudia el caso específico de una afectación a un sujeto de datos por parte de una empresa de telecomunicaciones, aplicando para tal fin tanto los principios de la protección de datos planteados por la sentencia Nº 8996-02 como los razonamientos de anteriores sentencias (5802-99 y 04847-99).

Sentencia Nº 2007-10114

A lo largo de ella la Sala examina el derecho al olvido a la luz del derecho de autodeterminación informativa, basándose para ello en jurisprudencia ya

establecida (mencionando entre otras las sentencias 04847-99, 2000-01119 y 2007-006793) e incluso extendiendo su análisis al derecho al olvido en materia civil, con tal de justificar su razonamiento.

*Etapa de Remisión de Asuntos de Autodeterminación Informativa a la PRODHAB*

Última y más reciente de las etapas señaladas por Carvajal Pérez, la *etapa de remisión de asuntos de autodeterminación informativa a la PRODHAB* se caracteriza, tal como su nombre lo indica, por un distanciamiento cada vez mayor de parte de la Sala Constitucional del tema de la protección de datos personales y el derecho a la autodeterminación Informativa, a favor de la vía administrativa creada con la entrada en vigencia de la Ley Nº 8968 para la protección de la persona frente al tratamiento de sus datos personales y su reglamento.

Esta etapa cuenta a la fecha con una sola resolución representativa (pues sus contenidos son por lo general reiterados a lo largo de cualquier recurso relacionado con el tema presentado ante la Sala):

Sentencia Nº 2013-15183

Establece esta sentencia que si bien la Sala Constitucional admitió desde su creación múltiples recursos relacionados con el derecho a la autodeterminación informativa, la creación de la PRODHAB y de un procedimiento administrativo especializado para el tratamiento de los casos relacionados con la protección

de los datos personales de los habitantes del país, le han llevado a la reponderación de la admisibilidad de dichos casos.

Así las cosas, la Sala actualmente afirma que *"ahora los habitantes cuentan con un mecanismo célere, oportuno y especializado para garantizar su derecho a la autodeterminación informativa en relación con su vida o actividades privadas y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes (ver artículo 1 de la ley No. 8968). Así las cosas, en tesis de principio, esta Sala remite a esa instancia administrativa los asuntos en donde se alegue la violación del derecho de comentario, reservándose el conocimiento, únicamente, de aquellos asuntos en los que habiendo acudido ante la Agencia de Protección de Datos de los Habitantes, no se haya encontrado amparo a ese derecho"*(Sala Constitucional de la Corte Suprema de Justicia, 2013).

### *Leyes*

#### *Ley Nº 63 "Código Civil"*

Emitido por Ley Nº 30 del 19 de abril de 1885 y vigente desde el primero de enero de 1888, nuestro Código Civil establece los fundamentos de la legislación positiva civil costarricense. Dentro de sus elementos más significativos para el tema en estudio se encuentra el hecho de que dedica la totalidad del título segundo de su libro primero al

establecimiento de los derechos de la personalidad y nombre de las personas, de conformidad con la tradición civilista mencionada a lo largo del capítulo primero.

Dentro de sus disposiciones fundamentales se encuentran las siguientes:

- Artículo 44 – Excluye del comercio a los derechos de la personalidad.
- Artículo 46 – Permite a toda persona negarse a ser sometida a exámenes o tratamientos médicos (con ciertas excepciones), pero establece también la posibilidad de que con base en tal negación sean considerados como probados los hechos controvertidos que se intentaban probar en un proceso judicial.
- Artículo 47: Prohíbe la publicación, reproducción, exposición y venta[286] sin consentimiento de la fotografía o la imagen de una persona (excepto cuando esta se justifique por la notoriedad o función pública del individuo, su interés público, o que tengan lugar en público). Asimismo el siguiente artículo permite que, en caso de darse estas situaciones, el afectado pueda solicitar la suspensión de dichas acciones.
- Artículo 59 – Reconoce el *"derecho a obtener indemnización por daño moral en los casos de lesión a los derechos de la personalidad" (Asamblea Legislativa de la República de Costa Rica, 1888).*

*Ley Nº 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales*

[286] Y prohíbe totalmente la realización de estas acciones con respecto a "fotografías con roles estereotipados que refuercen actitudes discriminantes hacia sectores sociales" (Asamblea Legislativa de la República de Costa Rica, 1888).

Sin duda uno de los cuerpos normativos más relevantes para la presente investigación, la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, fue aprobada por la Asamblea Legislativa el 7 de julio de 2012.

Generada como resultado del largo proceso de discusión y evolución[287] relativo al reconocimiento de la problemática del tratamiento de los datos personales en el país, la Ley tiene como objetivo fundamental *"garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes"* (Asamblea Legislativa de la República de Costa Rica, 2011).

La ley se encuentra dividida en cinco capítulos que versan sobre las disposiciones generales aplicables a la Ley, los principios y derechos básicos para la protección de datos personales, las transferencias de datos personales, la agencia de protección de datos de los habitantes y los procedimientos, respectivamente.

El primer capítulo de la Ley se dedica a realizar definiciones fundamentales sobre el tema de la protección de datos a la vez que aclara su objetivo, fin y ámbito de aplicación. Con respecto a este último punto la ley afirma su necesaria aplicación *"a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos"* (Asamblea Legislativa

[287] Existen en el país múltiples obras literarias y tesis de grado que abordan los detalles relativos a la historia de los proyectos legislativos que culminaron con la creación de nuestra actual ley Nº 8968 por lo que recomiendo al lector que desee un mayor grado de detalle comenzar su investigación por la lectura de: (Chirino & Carvajal, 2005).

de la República de Costa Rica, 2011), excluyendo explícitamente los datos mantenidos con fines exclusivamente internos, personales o domésticos que no sean comercializados de manera alguna.

Más adelante, la Ley dedica su segundo capítulo a la declaración de una serie de derechos elementales para la protección de datos personales que no habían podido ser encontrados en otras fuentes normativas nacionales hasta la fecha. El primero de estos derechos puede ser encontrado en el artículo cuarto de la Ley, titulado *Autodeterminación informativa*, a lo largo del cual se declara que *"toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección. Se reconoce también la autodeterminación informativa como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad ([288]), evitando que se propicien acciones discriminatorias" (Asamblea Legislativa de la República de Costa Rica, 2011).*

La ley reconoce seis excepciones válidas al derecho de autodeterminación informativa del ciudadano[289], a saber: a) la seguridad del Estado; b) la seguridad y el ejercicio de la autoridad pública[290]; c) la prevención[291], persecución, investigación y represión de las

[288] Personalmente considero que esta mención al *derecho a la privacidad* resulta incomprensible en el contexto del derecho constitucional costarricense pues nuestra Constitución Política menciona únicamente el derecho a la Intimidad. El término privacidad es un anglicismo que hace alusión al *privacy anglosajón*, el cual posee algunos matices distintos de los encontrados en el derecho a la intimidad (ver segundo capítulo de la presente investigación).

[289] Elemento que debemos señalar pues, a pesar de dirigirse a tutelar a los habitantes, la ley plantea excepciones únicamente para el ciudadano, lo cual, de ser aplicado de manera textual podría degenerar en tratos discriminatorios para los ciudadanos costarricenses.

[290] Excepción que a criterio de este investigador debe ser examinada con gran detalle dado su potencial abuso por parte de la administración pública.

[291] Resulta de cuidado en este punto el hecho de que no se señale la orden judicial como requisito para la limitación del derecho de autodeterminación informativa en estos casos y que, al contrario, se incluya la posibilidad de limitar dicho derecho con miras a la prevención de infracciones penales y de la deontología, arrogándose en potencia a los proveedores de servicio, a los entes de investigación judicial

infracciones penales o las infracciones a la deontología en las profesiones; d) los fines estadísticos o de investigación científica sin riesgo de identificación de los interesados; e) la adecuada prestación de los servicios públicos; y f) la eficaz actividad ordinaria de la administración por parte de las autoridades oficiales[292].

A continuación detalla este segundo capítulo los varios principios que acompañarán a la autodeterminación informativa en nuestro país, mencionando expresamente tanto el principio de consentimiento informado y las formalidades necesarias para el otorgamiento de dicho consenso así como el principio de calidad de la información, el cual se verá marcado por la necesidad de actualidad, veracidad, exactitud y adecuación al fin. Asimismo, menciona también este capítulo los derechos de acceso a la información[293], rectificación, actualización, cancelación, eliminación y confidencialidad de sus datos personales como *derechos que asisten a la persona*.

La sección segunda del capítulo segundo de la Ley Nº 8689 resultará de especial relevancia para nuestra investigación en tanto ella detalla las categorías especiales del

---

y a los colegios profesionales la capacidad de extrapolar información a partir de los datos y metadatos en su poder con miras a la prevención de hechos aún indeterminados.
(Ver capítulo segundo de la presente investigación en el cual se menciona, entre otros detalles, las tendencias recientes hacia el examen profundo de los paquetes transmitidos en las telecomunicaciones, las cuales permitirán llevar a cabo estas prácticas que según jurisprudencia internacional no constituyen necesariamente violación al secreto de las comunicaciones y por ende no requieren de órdenes judiciales para ser llevadas a cabo.)

[292] Nuevamente, debemos señalar el potencial de abuso de esta excepción en tanto la información recopilada a lo largo del segundo capítulo de la presente investigación pone en evidencia la facilidad con que los datos adquiridos por la administración pública con miras a garantizar la eficacia de su actividad ordinaria pueden poner en riesgo la integridad de la personalidad virtual (y física) del interesado.
Tal como discutimos a lo largo del punto relacionado con la traición por datos de localización, la adquisición indiscriminada de datos y metadatos aparentemente circunstanciales por parte de la administración puede llegar a identificar al individuo al punto que se vulneren incluso las precauciones que este adopte (y que lastimosamente en la mayor parte de los casos no son muy sofisticadas) en materia de seguridad informática.

[293] Que en nuestro país garantizará al interesado su capacidad de obtener en intervalos razonables la información de manera detallada y clara, por escrito sea de manera física o electrónica, a la vez que le faculta para "tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales" (Asamblea Legislativa de la República de Costa Rica, 2011).

tratamiento de los datos reconocidas en Costa Rica. Específicamente la Ley menciona cuatro categorías de datos personales, a saber:

- Datos sensibles: Se trata de aquellos datos *"que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, así como los relativos a la salud, la vida y la orientación sexual, entre otros" (Asamblea Legislativa de la República de Costa Rica, 2011)* cuyo tratamiento se encontrará prohibido[294] en el país. Esta prohibición posee según la ley cuatro excepciones:
    - el interés vital del interesado;
    - que dichos datos hayan sido hechos públicos voluntariamente[295];
    - que el tratamiento sea efectuado por organismos cuya finalidad sea afín al carácter de los datos tratados siempre que sus datos se refieran a sus miembros y no sean comunicados a terceros sin consentimiento del interesado; y
    - que el tratamiento resulte necesario para la prevención o tratamiento médico por parte de un profesional de la salud sujeto al secreto profesional.

[294] Se debe señalar que lastimosamente no extiende su ámbito de aplicación nuestra ley también a los metadatos que pueden señalar en su conjunto la misma información que los datos sensibles.

[295] Con respecto a los datos publicados voluntariamente por los interesados debemos señalar que los mismos deberían encontrarse sujetos también al ejercicio voluntario del derecho al olvido. Asimismo, el carácter voluntario de la liberación de datos debe ser acompañado por una declaración de consentimiento informado del tratamiento que cumpla con los parámetros del derecho de acceso a la información y permita al interesado manifestar su consentimiento sobre el uso que se pueda dar a esos datos (incluyéndose por supuesto elementos que permitan al sujeto decidir sobre la capacidad del administrador de la base de datos de vender, ceder, transmitir o comunicar de cualquier manera dichos datos).
En este punto resulta necesario recordar la existencia de propuestas como la "Chain-Link Confidentiality" (Hartzog, 2012) que proponen restricciones contractuales interconectadas sobre el uso de la información personal y que permiten al individuo mantener el control de su información una vez que esta ha sido liberada de manera voluntaria.

- Datos personales de acceso restringido: Son datos que *"aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Su tratamiento será permitido únicamente para fines públicos o si se cuenta con el consentimiento expreso del titular" (Asamblea Legislativa de la República de Costa Rica, 2011).*
- Datos personales de acceso irrestricto: Contenidos en bases de datos públicas de acceso general según la ley y que cumplen con las finalidades para las que fueran recabados.[296]
- Datos referentes al comportamiento crediticio: Regidos por las normas del sistema financiero nacional, buscan garantizar un grado de riesgo aceptable para las entidades financieras sin irrespetar los fines de la ley o los derechos de los interesados.

Finalmente el capítulo se refiere a la seguridad y confidencialidad debidas en el tratamiento de los datos. En materia de seguridad, la Ley dirige a todo responsable de bases de datos a adoptar las medidas técnicas y organizativas para asegurar la seguridad física y lógica (de conformidad con los últimos desarrollos tecnológicos) de los datos, pudiendo emitir y registrar sus protocolos de actuación ante PRODHAB [297].

[296] Al respecto de estos datos, aclara la ley que "No se considerarán contemplados en esta categoría: la dirección exacta de la residencia, excepto si su uso es producto de un mandato, citación o notificación administrativa o judicial, o bien, de una operación bancaria o financiera, la fotografía, los números de teléfono privados y otros de igual naturaleza cuyo tratamiento pueda afectar los derechos y los intereses de la persona titular" (Asamblea Legislativa de la República de Costa Rica, 2011).

[297] En este punto, vale mencionar que el artículo 12 la ley establece que "Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, el almacenamiento y el uso de datos personales, podrán emitir un protocolo de actuación en el cual establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta ley" (Asamblea Legislativa de la República de Costa Rica, 2011).
Debe enfatizarse en este caso el carácter discrecional de la emisión del protocolo de actuación, con lo cual nuestra ley se separa de los ejemplos internacionales que obligan a todo responsable de emitir, registrar y cumplir con dicho protocolo, contando para ello con profesionales dedicados a verificar constantemente dicho cumplimiento.

Por otro lado, la Ley impone la obligación de confidencialidad a los responsables (y a todos quienes intervengan en el tratamiento) a guardar secreto profesional o funcional aún a posteriori.

El capítulo tercero contiene las únicas referencias realizadas por nuestra ley a las transferencias internacionales de datos personales. En un escueto artículo catorce, la Ley 8968 afirma que: *"Los responsables de las bases de datos, públicas o privadas, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley" (Asamblea Legislativa de la República de Costa Rica, 2011).*[298]

A continuación, el capítulo cuarto de la Ley crea la Agencia de Protección de Datos de los Habitantes (PRODHAB)[299], a la cual impone atribuciones específicas como lo son el registro de archivos y bases de datos así como tareas de divulgación, educación y comunicación en favor de los administrados. La PRODHAB deberá por ello promover el manejo adecuado de los datos personales en la sociedad costarricense e impulsar entre las personas y empresas que recolecten datos personales, la adopción de prácticas y protocolos de actuación acordes con la protección de dicha información.

Finalmente, la ley dedica su capítulo quinto a la disposición de varios aspectos procedimentales en los cuales se detallan temas como la intervención en archivos y

[298] Resultará evidente al lector que es aquí donde encontraremos una mayor disonancia entre la ley Nº 8968 y la realidad puesta en evidencia a lo largo de nuestro estudio de las telecomunicaciones convergentes.
A lo largo de la presente investigación hemos podido observar la suma seriedad con la cual el tema de las transferencias internacionales ha sido adoptado por las diversas normativas internacionales. Ante esta circunstancia, el articulo catorce de nuestra ley se nos presenta como una manifestación vibrante de la obsolescencia de nuestra "novedosa" normativa, la cual ignora el carácter necesariamente transnacional de las telecomunicaciones convergentes (populares a lo largo del mundo desde hace ya varios años) que no hará más que crecer en el futuro.
[299] Ya estudiada en el principio del presente capítulo.

bases de datos; los procedimientos sancionatorios[300], los procedimientos internos y los cánones aplicables a las bases de datos registradas.

*Ley Nº 7975 "de Información No Divulgada"*

Dirigida, entre otros fines, a proteger la información no divulgada relacionada con los secretos comerciales e industriales, esta ley se encuentra tangencialmente relacionada con nuestro tema de estudio en tanto sus disposiciones resultan relevantes para la protección de datos relevantes a personas jurídicas en Costa Rica.

Con miras a lograr tales fines, la Ley 7975 incluye dentro de su ámbito de protección los secretos comerciales e industriales guardados confidencialmente por personas físicas o jurídicas, con miras a impedir la divulgación de información legítimamente bajo su control o el uso sin consentimiento de esta de manera contraria a los usos comerciales honestos.

Excluyendo de su ámbito de protección aquella información que se encuentre dentro del dominio público, resulte evidente para un técnico versado en la materia con base en información disponible de previo o deba ser divulgada por disposición legal o judicial, la Ley establece que la información por proteger se ajuste a los siguientes requisitos (Asamblea Legislativa de la República de Costa Rica, 2000):

[300] Definidos a lo largo de los artículos 28 a 31 de la ley. Dentro de sus disposiciones encontramos dos elementos dignos de mención: a) asigna como falta leve la transferencia de datos por "mecanismos inseguros", y b) menciona en dos ocasiones el artículo tercero de la ley, declarando como falta grave la transferencia no autorizada de datos a empresas o personas en el país y como falta gravísima la transferencia no autorizada a terceros países.

1) Sea secreta: no sea conocida ni fácilmente accesible.
2) Esté legalmente bajo el control de una persona que haya adoptado medidas razonables y proporcionales para mantenerla secreta.
3) Tenga un valor comercial por su carácter de secreta.

*Ley Nº 4573 "Código Penal"*

El Código Penal constituye la base de la legislación penal positiva de nuestro país, vigente desde el 15 de noviembre de 1970 y reformado numerosas veces. Aparte de los elementos examinados a lo largo del análisis de la Ley 9048, este código contiene en su actual versión una buena cantidad de disposiciones que resultan relevantes para el presente tema de estudio, dentro de las cuales pueden encontrarse las siguientes:

- Establece algunas regulaciones relevantes al tema de la persecución extraterritorial de hechos punibles cometidos en el extranjero cuando estos: *"Produzcan o puedan producir sus resultados en todo o en parte, en el territorio nacional; (…) Se perpetraren contra de algún costarricense o sus derechos; (o) hayan sido cometidos por algún costarricense" (Asamblea Legislativa de la República de Costa Rica, 1970),* para los cuales permite la aplicación de la ley costarricense.

  Asimismo, reconoce en su artículo 7 la posibilidad de penar, con independencia de las disposiciones vigentes en el lugar de la comisión del hecho punible y la nacionalidad del autor, a quienes cometan *"hechos punibles contra los derechos humanos y el Derecho internacional humanitario, previstos en los tratados suscritos*

*por Costa Rica o este Código" (Asamblea Legislativa de la República de Costa Rica, 1970).*

- Dedica su título IV al tratamiento de los delitos contra el ámbito de intimidad, se encuentran en este tanto las reformas ya estudiadas que fuesen promovidas por la Ley 9048, como las siguientes disposiciones:
    - Artículo 198 - Castiga con prisión de uno a tres años[301] a quien grabe, escuche o instale aparatos, instrumentos o sus partes con el fin de interceptar o impedir las comunicaciones orales o escritas, estén estas destinadas o no lo estén al público.
    - Artículo 201 – Reprime con prisión de seis meses a un año el uso indebido de correspondencia que hubiese sido substraída o reproducida.
    - Artículo 202 – Reprime con treinta a sesenta días multa[302] a quien haga públicas piezas de correspondencia, papeles o grabaciones no destinadas a la publicidad sin la debida autorización (aunque le hubieren sido dirigidas).
    - Artículo 203 – Reprime con prisión de un mes a un año o de treinta a cien días multa[303] a quien revele sin justa causa un secreto cuya divulgación pueda causar daño del que haya tenido noticia por razón de

[301] El artículo 200 agrava la pena (de dos a seis años) si la acción se perpetra por funcionarios públicos; por quien ejecute el hecho gracias a su relación con el ente encargado de las comunicaciones; o cuando el autor publique la información o el juez determine que esta tiene carácter privado.
[302] O con treinta a cien días multa si la información tuviese carácter privado, aun cuando su propalación no causare perjuicio.
[303] "Si se tratare de un funcionario público o un profesional se impondrá, además inhabilitación para el ejercicio de cargos y oficios públicos, o de profesiones titulares, de seis meses a dos años" (Asamblea Legislativa de la República de Costa Rica, 1970).

su estado, oficio, empleo, profesión o arte (Asamblea Legislativa de la República de Costa Rica, 1970).

- Artículo 322 bis – El cual pena a quien difunda por sí o cualquier medio *"información confidencial relacionada con personas sujetas a medidas de protección en el programa de víctimas y testigos" (Asamblea Legislativa de la República de Costa Rica, 1970).*
- Artículo 346 – Castiga a aquel funcionario público que divulgue hechos, actuaciones o documentos clasificados por ley como secretos.

*Ley Nº 9048 "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del título VII del Código Penal"*

Generada con miras a reformar y actualizar la sección relativa a los delitos informáticos y conexos del título VII de nuestro Código Penal, la Ley Nº 9048 (mejor conocida como "ley de delitos informáticos") fue adoptada por nuestro país el 10 de julio del 2012 y entró en vigencia el 06 de noviembre de ese mismo año. Fundamentada en convenios internacionales tales como el Convenio de Budapest sobre Ciberdelincuencia, la ley de delitos informáticos sanciona a aquellas personas que hacen un uso irresponsable y doloso de las tecnologías de la información y la comunicación con miras a perjudicar a otros.

A lo largo de sus tres artículos, la ley reforma los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley Nº 4573, Código Penal, de 4 de mayo de 1970. Dentro de

los artículos reformados, resultan relevantes para la presente investigación los siguientes:

- Artículo 196.- Violación de correspondencia o comunicaciones: artículo que reprime con pena de tres a seis años a quien *"con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización, se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidos a otra persona" (Asamblea Legislativa de la República de Costa Rica, 2012).* Este artículo incluye penas mayores (cuatro a ocho años) si quien realiza la violación es el encargado de los documentos o de la administración o soporte del sistema o red informática.
- Artículo 196 bis.- Violación de datos personales: De especial relevancia para la presente investigación por evidentes razones, este artículo sanciona con penas de tres a seis años a quien *"en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos" (Asamblea Legislativa de la República de Costa Rica, 2012).* Asimismo, la Ley castiga con mayor severidad (cuatro a ocho años de prisión) estas conductas cuando sean realizadas por los administradores del sistema o personas con acceso a este; cuando los datos afectados sean públicos o se encuentren en bases de datos públicas; cuando la

información personal haga referencia a menores de edad o incapaces y cuando se hallan visto afectados datos sensibles.

- Artículo 217 bis.- Estafa informática: impone una sanción de tres a seis[304] años contra quien manipule o influya en el ingreso, procesamiento o resultado de sistemas automatizados de información *"ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro" (Asamblea Legislativa de la República de Costa Rica, 2012).*
- Artículo 229 bis.- Daño informático: artículo que castiga a quien suprima, modifique o destruya la información contenida en un sistema o red informático o en contenedores ópticos, electrónicos o magnéticos, castigando con especial rigurosidad a quien dañe información insustituible o irrecuperable.
- Artículo 234.- Facilitación del delito informático: el cual castiga a quien facilite los medios para la consecución de un delito informático.

Mediante la reforma de los artículos supracitados, las reformas producidas por esta ley no solamente refuerzan los medios existentes para la sanción de conductas ilícitas que puedan afectar los datos personales y el derecho de autodeterminación informativa, sino que también posibilitaron la aplicación de la Convención de Palermo, que como

[304] O de cinco a diez años si las conductas fueran cometidas contra un sistema de información público, sistema de información bancario o de entidades financieras, y cuando el autor es también administrador o encargado de dar soporte al sistema.

podrá recordar el lector era solamente aplicable a aquellos delitos castigados con penas mayores a cuatro años de prisión.

*Ley Nº 9135 "Reforma de los artículos 196, 196 bis, 230, 293, y 295 y adición del artículo 167 bis al Código Penal"*

Dirigida a subsanar algunos defectos en la redacción de los artículos 196, 196 bis, 230, 293, y 295 ante los movimientos populares que tachaban a la Ley Nº 9048 de ser una "ley mordaza", la Ley Nº 9135 fue aprobada por la Asamblea Legislativa el 24 de abril de 2013; incluye algunos cambios sutiles pero importantes a nuestro Código Penal, a la vez que incluye un artículo (el 167 bis) dirigido a penalizar la seducción o encuentros con menores por medios electrónicos.

Específicamente, los cambios realizados a los artículos atinentes a la protección de datos personales son los siguientes:

- Artículo 196: extiende la sanción originalmente planteada por la ley Nº 9048 a *"quien, con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público. La misma pena se impondrá a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores" (Asamblea Legislativa de la República de Costa Rica, 2013).*
- Artículo 196 bis: elimina el punto b) incluido en este artículo por la Ley Nº 9048 relativo al aumento de la pena *"cuando los datos sean de carácter público o estén*

*contenidos en bases de datos públicas" (Asamblea Legislativa de la República de Costa Rica, 2012).*

- Artículo 230: Modifica las disposiciones de la Ley Nº 9048 con tal de castigar la suplantación de identidad de personas físicas, jurídicas e incluso de marcas comerciales en redes sociales, sitios de internet y otros medios electrónicos y tecnológicos de información.

  Asimismo, elimina las disposiciones de su antecesora respecto al castigo asignado a quien cause perjuicios utilizando identidades falsas o inexistentes (en tanto se considera que esta disposición limita seriamente el derecho al anonimato) y elimina también el segundo párrafo del artículo (referente al castigo mayor para quien afecte a menores de edad e incapaces).

*Ley Nº 7425 "sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones"*

Tal como su nombre lo indica, la Ley Nº 7425 del 08 de septiembre de 1994 se dedica a regular el registro, secuestro y examen de documentos privados e intervención de las comunicaciones en nuestro país, las cuales deberán ser ordenadas por jueces de la República en el marco de la debida legalidad, razonabilidad y respeto a los derechos fundamentales de los sujetos afectados.

La ley consta de cinco capítulos; los dos primeros son especialmente relevantes para para la presente investigación.

El primer capítulo realiza las disposiciones concernientes al registro, secuestro y examen de documentos privados en nuestro país, los cuales son definidos como cualquier forma de registrar información de carácter privado, utilizada con carácter representativo o declarativo, para ilustrar o comprobar algo[305].

Por su parte, el segundo capítulo se refiere única y exclusivamente a la intervención de las comunicaciones y dentro de sus doce artículos, dos resultan de interés para esta investigación:

- Artículo 9: Determina los requisitos para la autorización de intervenciones y, en su parte fundamental, reza lo siguiente: *"Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de los siguientes delitos: secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, tráfico de personas y tráfico de personas para comercializar sus órganos; homicidio calificado; genocidio, terrorismo y los delitos previstos en la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas, Nº 8204, del 26 de diciembre del 2001"* (Asamblea Legislativa de la República de Costa Rica, 1994).

[305] La relevancia de este capítulo en el contexto del mundo de las telecomunicaciones convergentes se ve explicada al concordar el concepto de documento privado manifestado en la ley Nº 7475 con el principio de equivalencia funcional reconocido por el artículo tercero de la Ley Nº 8454 de Certificados, Firmas Digitales y Documentos Electrónicos, el cual afirma que "Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos."
Con base en estas disposiciones, todo juez de nuestro país posee la potestad de ordenar el registro, secuestro y examen de documentos contenidos en medios electrónicos o digitales de cualquier tipo.

- Artículo 14: Permite expresamente el empleo de todos los medios técnicos pertinentes[306], encaminados a conocer y a conservar las comunicaciones orales o escritas que se produzcan.

*Ley Nº 8754 contra la Delincuencia Organizada*

Aprobada por la Asamblea Legislativa el 22 de julio de 2009, la Ley contra la Delincuencia Organizada No. 8754 del 22 de julio de 2009, establece un conjunto de disposiciones legales dirigidas a combatir activamente todo grupo estructurado de personas dirigido a cometer delitos graves de manera concertada.

Esta ley es digna de mención en la presente investigación en tanto su artículo 11 crea la *Plataforma de Información Policial*; un sistema que vincula todos los cuerpos policiales del país y les permite compartir información de sus registros, bases de datos, expedientes electrónicos, redes internacionales e inteligencia policial con tal de impulsar la eficiencia y eficacia de todas sus investigaciones.

Dentro de sus postulados más importantes, el artículo establece que:

*"Salvo en los casos en que se requiera orden del juez para accederlos, todos los registros, las bases de datos, los expedientes de los órganos y las entidades estatales, las instituciones autónomas y las corporaciones municipales podrán ser accedidos por la Plataforma de Información Policial, sin necesidad de orden judicial.*

[306] Con lo cual se permite que el juez requiera de los operadores de servicios de telecomunicaciones los datos de tráfico y localización que posean en sus bases de datos.

*Cuando el acceso a los datos solamente pueda realizarse con la orden del juez, únicamente podrán imponerse de ellos los policías o investigadores designados previamente, así como los fiscales a cargo del caso y los jueces a quienes corresponda dictar algún auto o sentencia de ese caso; cuando la misma información se requiera en otro proceso, esta no podrá conocerse o compartirse sin la autorización previa de la autoridad judicial. Quienes conozcan tales datos legalmente, deberán guardar secreto de ellos y solamente podrán referirlos en declaraciones, informes o actuaciones necesarias e indispensables del proceso.*

*El director del Organismo de Investigación Judicial será el responsable por los aspectos ejecutivos de la Plataforma y determinará los niveles de acceso a la información, y los cuerpos policiales y de investigación que podrán acceder a ella; para estos efectos, elaborará un protocolo de acceso y uso de la información contenida en dicha Plataforma.*

*Respecto de la información, cualquier fuga que perjudique los resultados de las investigaciones o el uso ilegal de esta en perjuicio del investigado o de otras personas, será responsabilidad directa del funcionario o los funcionarios involucrados"* (Asamblea Legislativa de la República de Costa Rica, 2009).

### *Ley Nº 6227 "Ley General de la Administración Pública"*

De gran importancia dada su evidente relación con todas las actuaciones públicas, la Ley General de la Administración Pública se relaciona especialmente con la protección de datos personales en tanto es referenciada directamente por el los artículos 27 y 58 del Reglamento a la Ley Nº 8968, que establecen la necesaria aplicación de los

principios del proceso administrativo[307] establecidos en el libro segundo de la Ley Nº 6277. Asimismo, resulta importante mencionar tres artículos de la Ley como relevantes para el tema en cuestión, a saber:

- Artículo 272: Establece dentro de las formalidades de los procedimientos administrativos la capacidad de *"Las partes y sus representantes, y cualquier abogado" (Asamblea Legislativa de la República de Costa Rica, 1978)* a examinar, leer y copiar piezas del expediente.
- Artículo 273: Limita el acceso otorgado por el artículo anterior para aquellas piezas del expediente *"cuyo conocimiento pueda comprometer secretos de Estado o información confidencial de la contraparte o, en general, cuando el examen de dichas piezas confiera a la parte un privilegió indebido o una oportunidad para dañar ilegítimamente a la Administración, a la contraparte o a terceros, dentro o fuera del expediente" (Asamblea Legislativa de la República de Costa Rica, 1978).*
- Artículo 310: Limita a las partes y sus representantes y abogados la comparecencia en el acto, pero posibilita a la Administración a permitir *"la presencia de estudiantes, profesores o científicos, quienes asistirán obligados por el secreto profesional" (Asamblea Legislativa de la República de Costa Rica, 1978).*

*Ley Nº 17 "Ley Constitutiva de la Caja Costarricense del Seguro Social"*

[307] Y la aplicación supletoria de otras disposiciones relevantes para lo no previsto expresamente por la ley en tanto sean compatibles con su finalidad.

La Ley Nº 17 del 22 de octubre de 1943 resulta de interés para esta investigación en tanto contiene algunas disposiciones relevantes para la información, relacionada con el cumplimiento de las obligaciones sociales por ella impuestas. Específicamente se trata de los siguientes artículos:

- Artículo 20: Referido a la inspección del cumplimiento de la ley y sus reglamentos, para lo cual asigna carácter de confidencial a toda la información relacionada y establece que *"su divulgación a terceros particulares o su mala utilización serán consideradas como falta grave del funcionario responsable y acarrearán, en su contra, las consecuencias administrativas, disciplinarias y judiciales que correspondan, incluida su inmediata separación del cargo"* (Asamblea Legislativa de la República de Costa Rica, 1943).
- Artículo 54: Artículo relacionado con la capacidad de denunciar infracciones de cualquier persona, así como al derecho de acceso a la información que poseen las organizaciones de trabajadores o patronos y los asegurados ante la Junta Directiva de la Caja, la cual deberá cumplir, siempre y cuando no existan disposiciones legales de confidencialidad que se lo impidan.
- Artículo 63: Prohíbe a la Gerencia (salvo autorización expresa de la Directiva), la divulgación o suministro a particulares *"los datos y hechos referentes a asegurados y patronos de que tenga conocimiento en virtud del ejercicio de sus funciones; pero podrá publicar cualquier información estadística o de otra índole que no se refiera a ningún asegurado o patrono en especial"* (Asamblea Legislativa de la República de Costa Rica, 1943).

- Artículo 74: En él se reconoce la necesidad de contar con bases de datos conjuntas y sistemas de control y verificación que faciliten el control del cumplimiento del pago de las obligaciones con la seguridad social.

*Ley Nº 9162 "Expediente Digital Único de Salud"*

Promulgada por la Asamblea Legislativa el 26 agosto de 2013, la Ley Nº 9162 se dirige a establecer en nuestro país el ámbito y los mecanismos de acción necesarios para el desarrollo de un sistema de expediente digital único de salud, entendido este como *"el repositorio de los datos del paciente en formato digital, que se almacenan e intercambian de manera segura y puede ser accedido por múltiples usuarios autorizados. Contiene información retrospectiva, concurrente y prospectiva, y su principal propósito es soportar de manera continua, eficiente, con calidad e integralidad la atención de cuidados de salud" (Asamblea Legislativa de la República de Costa Rica, 2013).*

Con miras a lograr su fin, la Ley no solamente declara de interés público todas las fases del proyecto, sino que además designa dentro de sus objetivos principales *"que cada persona tenga un expediente electrónico con la información de toda la historia de atención médica con las características de disponibilidad, integridad y confidencialidad" (Asamblea Legislativa de la República de Costa Rica, 2013)*. Asimismo, la Ley procura la promoción de la interoperabilidad de la información, el procesamiento, la confidencialidad, la seguridad y el uso de estándares y protocolos interinstitucionales de conformidad con los principios del consentimiento informado y la autodeterminación informativa.

A lo largo de su articulado la ley no solamente establece las disposiciones administrativas necesarias para la el correcto planteamiento, diseño, ejecución, implementación y operación del sistema; también determina las características claves para ser adoptadas por la solución tecnológica por ser desarrollada. Específicamente, estas características serán:

- Interoperabilidad[308]
- Mejores prácticas[309]
- Seguridad[310]
- Escalabilidad
- Usabilidad
- Productividad y Calidad
- Portabilidad[311]
- Integridad[312]
- Identificación única[313]
- Acceso único
- Trazabilidad

[308] Característica dirigida a garantizar el efectivo y transparente intercambio de información.
[309] Que requiere que las soluciones tecnológicas se guíen por los más altos parámetros técnicos y médicos.
[310] Debiendo cumplir el expediente digital con estrictos criterios tecnológicos, científicos, éticos y administrativos *"en aras de garantizar la integridad, confidencialidad y disponibilidad en el uso, manejo, archivo, conservación y propiedad de los datos"* (Asamblea Legislativa de la República de Costa Rica, 2013)
[311] La mención de esta característica abre la posibilidad de que todo usuario lleve consigo la información de su expediente clínico mediante el uso de dispositivos electrónicos.
[312] Procurando mantener la calidad y confiabilidad de los datos clínicos del paciente.
[313] La identificación unívoca de los usuarios del expediente digital constituye una de las necesidades fundamentales del proceso de implementación en tanto es requisito fundamental para el cumplimiento pleno de los principios de confidencialidad y veracidad.

- Cumplimiento de los requerimientos necesarios para la prestación de servicios de salud.

Finalmente, la Ley dedica su onceavo artículo a la protección de la información privada, en el cual se establece expresamente el carácter sensible de la totalidad de la información contenida en el expediente digital único; se obliga al encargado de las bases de datos a guardar el secreto profesional y a la adopción de las mayores medidas técnicas y de organización; y se prohíbe el tratamiento de los datos sensibles[314].

*Ley Nº 4755 "Código de Normas y Procedimientos Tributarios"*

Vigente desde el 3 de mayo de 1971, el Código de Normas y Procedimientos Tributarios (también conocido como el Código Tributario) contiene múltiples disposiciones referentes a las obligaciones tributarias que el Estado exige en ejercicio de su poder de imperio, con el objeto de obtener recursos para el cumplimiento de sus fines.

Dentro de sus disposiciones más relevantes para este estudio, se encuentran las siguientes:

[314] Se debe recordar que la Ley Nº 8968 define tratamiento de datos personales como "cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, la organización, la conservación, la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción, entre otros." (Asamblea Legislativa de la República de Costa Rica, 2011).
En este contexto, la inclusión de una prohibición expresa al tratamiento de los datos personales en el artículo 11 de la Ley Nº 9162 resulta extraña en tanto pareciera contradecir el sentido de la Ley.

- Artículo 101: Relacionado con la publicidad de las normas y la jurisprudencia tributaria, este artículo reconoce la necesidad de omitir de las sentencias o resoluciones publicadas *"las referencias que puedan lesionar intereses particulares o la garantía del carácter confidencial de las informaciones" (Asamblea Legislativa de la República de Costa Rica, 1971)* dispuestas por el Código.
- Artículo 117: De suma relevancia para la protección de la información tributaria, este artículo afirma el carácter confidencial de toda aquella información obtenida de los contribuyentes por cualquier medio, por lo que prohíbe a la administración (incluyéndose en esta prohibición a múltiples instituciones relacionadas con el sector financiero) divulgar los datos de su conocimiento[315].
- Artículo 132: A lo largo de este se refleja la obligación de colaboración impuesta sobre los funcionarios y empleados públicos, a la vez que prohíbe a la Administración solicitar informaciones (y libera a los empleados de suministrarla) *"cuando en virtud de las disposiciones de este Código o de leyes especiales, las informaciones respectivas estén amparadas por la garantía de la confidencialidad" (Asamblea Legislativa de la República de Costa Rica, 1971).*

*Ley Nº 3284 "Código de Comercio"*

Dirigido a regir los actos y contratos en él determinados, aunque no sean comerciantes las personas que los ejecuten, nuestro Código de Comercio adquiere relevancia para

[315] E instituyéndose también las excepciones vigentes a esta confidencialidad.

esta investigación en tanto su artículo 615 comprende disposiciones específicamente dirigidas a asegurar el secreto bancario.

Específicamente afirma este artículo que: *"Las cuentas corrientes bancarias son inviolables y los bancos solo podrán suministrar información sobre ellas a solicitud o con autorización escrita del dueño, o por orden de autoridad judicial competente"* (Asamblea Legislativa de la República de Costa Rica, 1964).

### *Ley Nº 7732 "Ley Reguladora del Mercado de Valores"*

Con el objeto de regular los mercados de valores, las personas físicas o jurídicas que intervienen directa o indirectamente en ellos, los actos o contratos con ellos relacionados y los valores por ellos negociados, esta ley es creada por la Asamblea Legislativa el 17 de diciembre de 1997 y se relaciona con la presente investigación específicamente por medio de las disposiciones de dos de sus artículos, a saber:

- Artículo 108: La Ley regula la actuación de los participantes en el mercado y establece que *"La información que dichos participantes tengan de sus clientes será confidencial y no podrá ser usada en beneficio propio ni de terceros; tampoco para fines distintos de aquellos para los cuales fue solicitada" (Asamblea Legislativa de la República de Costa Rica, 1997)*.
- Artículo 151: Por medio de este se regula el intercambio de información entre la Superintendencia General de Valores y sus homólogos internacionales, estableciendo tanto la necesidad de reciprocidad en esta relación, como el que

los entes extranjeros se encuentren sujetos a prohibiciones de divulgación de información confidencial equiparables a las establecidas por esta ley.

*Ley Nº 7558 "Ley Orgánica del Banco Central de Costa Rica"*

En vigencia desde el tres de noviembre de 1995, la Ley Nº 7558 establece los aspectos fundamentales para el funcionamiento del Banco Central de Costa Rica, institución autónoma con patrimonio propio y personalidad jurídica, dirigida a mantener la estabilidad interna e interna de la moneda local. Sus principales disposiciones relevantes definen las reglas de manejo de la información en manos de la Superintendencia General de Entidades Financieras, y pueden ser encontradas en los siguientes artículos:

- Artículo 132: Prohíbe a toda persona física o jurídica que preste servicios a la Superintendencia el dar a conocer información sobre las entidades fiscalizadas[316] a la vez que prohíbe a los funcionarios expresar su criterio sobre la situación financiera de las entidades fiscalizadas.
- Artículo 133: Afirma la capacidad de la superintendencia de informar a las entidades fiscalizadas sobre la situación de los deudores del sistema financiero, de acuerdo con las reglas establecidas en los siguientes artículos. Asimismo, prohíbe en su punto d) a los funcionarios, empleados y administradores de las entidades fiscalizadas y de la Superintendencia, suministrar a terceros cualquier

[316] Salvo contadas excepciones establecidas por el artículo mismo.

dato de la información antes mencionada y castiga a quienes incumplan esta prohibición con penas de prisión y la destitución de su puesto laboral (Asamblea Legislativa de la República de Costa Rica, 1995).

Finalmente, asigna este artículo la responsabilidad de establecer las medidas internas necesarias para salvaguardar la confidencialidad de la información a la Superintendencia.

*Ley Nº 8131 "Ley de la Administración Financiera de la República y Presupuestos Públicos"*

Dirigida a regular el régimen económico-financiero de los órganos y entes administradores o custodios de fondos públicos, la Ley Nº 8131 aprobada el 16 de octubre de 2001 contiene también disposiciones relativas al manejo de bases de datos y de información confidencial (fundamentalmente información financiera), la cual se encuentra incluida dentro de los siguientes artículos:

- Artículo 28: Asigna al Ministro de Hacienda la rectoría del sistema de administración financiera y le encarga en su inciso d) el *"coordinar las actividades de procesamiento de datos, para efectos del cumplimiento de esta ley" (Asamblea Legislativa de la República de Costa Rica, 2001).*
- Artículo 110: Clasifica en su inciso c) el suministro o empleo de información confidencial de cualquier carácter referente al Estado, entes públicos o particulares, como un hecho generador de responsabilidad administrativa.
- Artículo 111: En él son tipificadas las actividades que constituyen un delito informático por parte de los funcionarios públicos o particulares. De estas,

resultan especialmente relevantes las disposiciones de sus incisos a) *"Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido" (Asamblea Legislativa de la República de Costa Rica, 2001)* Y c) *"Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas" (Asamblea Legislativa de la República de Costa Rica, 2001)*.

- Artículo 125 relevante en tanto requiere del Ministerio de Hacienda el desarrollo de un *Sistema Integrado de Información* para el cumplimiento de la Ley y la sustitución de los soportes documentales tradicionales por digitales.

*Ley Nº 8656 "Ley Reguladora del Contrato de Seguros"*

Emitida por la Asamblea Legislativa el 17 de junio de 2011 con miras a establecer normas de carácter imperativo sobre los contratos de seguros adoptados en el país, la Ley Nº 8656 adquiere relevancia en tanto su artículo 21 se encuentra dedicado expresamente a la protección de datos. El artículo establece lo siguiente:

*"Artículo 21.- Protección de datos*

*La información que en virtud de la suscripción de contratos privados de seguros obtengan las entidades aseguradoras queda tutelada por el derecho a la intimidad y confidencialidad. Las entidades aseguradoras, sus subsidiarias, sus proveedores de servicios auxiliares, empresas subcontratadas, y su personal, tanto directivo como de planta, estarán obligados a guardar el deber de confidencialidad de la información frente a su cliente y solo quedará liberada de este deber mediante convenio escrito, diferente del contrato de seguro, donde se expresen los fines*

*de levantamiento de la confidencialidad y el alcance de diseminación de los datos. En igual sentido, quedan obligados los intermediarios de seguros, así como las personas físicas o jurídicas que realicen actividades destinadas a la promoción, la oferta y, en general, los actos dirigidos a la celebración de un contrato de seguros, su renovación o modificación y el asesoramiento que se preste en relación con esas contrataciones.*

*La inobservancia comprobada de este deber constituirá infracción muy grave, sancionable de conformidad con lo establecido por el artículo 37 de la Ley Reguladora del Mercado de Seguros.*

*Quedan a salvo del deber de confidencialidad los datos que sea necesario exponer ante cualquier autoridad competente. Queda prohibida la divulgación de datos no relacionados directamente con el conflicto.*

*La violación del derecho de confidencialidad será causa suficiente para que el propietario de los datos tenga derecho a ser resarcido por los daños y perjuicios que se le hubieran provocado, sin perjuicio de cualquier otra acción legal que corresponda" (Asamblea Legislativa de la República de Costa Rica, 2011)*.

### *Reglamentos*

#### *Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales*

Decretado por el Poder Ejecutivo el 30 de octubre de 2012 y vigente desde el 05 de marzo de 2013, el Decreto Ejecutivo 37544 reglamenta expresamente a la Ley Nº 8968. A lo largo de sus diez capítulos, el Reglamento establece una serie de disposiciones

relativas al consentimiento; los derechos de los titulares y su ejercicio; el tratamiento de los datos personales y las medidas de seguridad; la transferencia de datos personales; la inscripción del registro de bases de datos y ficheros ante la Agencia; la protección de derechos ante la Agencia; el procedimiento de cobro; el pago de los cánones; y la Agencia de protección de datos de los habitantes.

Dentro de sus elementos fundamentales se pueden recalcar los siguientes:

- Añade un número significativo de definiciones, siglas y acrónimos a los ya reconocidos por la Ley Nº 8968.
- Expresa una serie de requisitos en relación con el consentimiento informado exigido por la Ley Nº8968, dentro de los cuales se encuentra que la obtención del consentimiento sea libre, específico, informado, expreso, e individualizado.

  Más aún, exige la ley que dicho consentimiento debe cumplir con una serie de formalidades, eximiéndose de esta obligación cuando exista orden judicial o acuerdo de una comisión especial de investigación de la Asamblea Legislativa; se trate de datos personales de acceso irrestricto; o los datos deban ser entregados por disposición constitucional o legal.

  Finalmente, impone la carga de la prueba sobre el responsable de la base de datos, a la vez que reconoce tanto el derecho de revocación del consentimiento como el derecho al olvido para el titular de los datos personales[317].
- Define la autodeterminación informativa como *"el derecho fundamental de toda persona física, a conocer lo que conste sobre ella, sus bienes o derechos en cualquier*

[317] El cual se establece en diez años desde la fecha de ocurrencia de los hechos registrados, sin embargo el reglamento establece también que "en caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados los datos personales de su titular" (Poder Ejecutivo de la República de Costa Rica, 2013).

*base de datos, de toda naturaleza, pública o privada, el fin para el cual está siendo utilizada o recabada su información personal, así como exigir que sea rectificada, actualizada, complementada o suprimida, cuando la misma sea incorrecta o inexacta, o esté siendo empleada para un fin distinto del autorizado o del que legítimamente puede cumplir"* [318] *(Poder Ejecutivo de la República de Costa Rica, 2013).*

- Reitera la capacidad del titular o su representante de ejercer sus derechos, sin excluirse por ello unos u otros. Asimismo, exige de los responsables del tratamiento la puesta a disposición de los titulares de medios y trámites simples, con plazos cortos para tramitar la solicitud y el requisito de poner a disposición de los interesados los aspectos relativos a las condiciones, finalidad y generalidades de su tratamiento.
- Establece una serie de obligaciones respecto al tratamiento de los datos personales, dentro de las que se encuentra la definición de las medidas de seguridad relevantes; el establecimiento y documentación de procedimientos para la inclusión, modificación, bloqueo y supresión de los datos en el sitio o en la nube; establecer y respetar las condiciones del tratamiento en conformidad con lo aceptado por el titular.

[318] Con lo cual el reglamento adopta una posición evidentemente retrógrada con respecto al artículo cuatro de la Ley Nº 8968, el cual, como recordará el lector establece que este derecho "abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos (y) reconoce también la autodeterminación informativa como un derecho fundamental con el objeto de controlar el flujo de informaciones que conciernen a cada persona (…)" (Asamblea Legislativa de la República de Costa Rica, 2011).
Una breve comparación de ambos textos permitirá al lector comprender que, si bien es cierto que la Ley Nº 8968 reconoce efectivamente el acceso a la información y los derechos a la rectificación, actualización, complementación o supresión de la misma, el derecho de autodeterminación informativa plasmado en el reglamento no contempla el aspecto preventivo de este derecho, ignorando que el sujeto protegido por este derecho fundamental debe ser siempre capaz de controlar los flujos de información, no debiendo esperar a que la misma sea vulnerada para ejercer sus derechos fundamentales.

- Requiere que el responsable asegure el cumplimiento por parte de los intermediarios o proveedores de las medidas de seguridad mínimas. Asimismo, establece una serie de obligaciones para el encargado del tratamiento, dentro de las cuales se encuentra el deber de confidencialidad, la implementación de medidas de seguridad y protocolos de actuación; y la supresión de los datos una vez cumplida su relación jurídica con el responsable.
- Detalla lo que debe entenderse como protocolo mínimo de actuación, en los cuales deben incluirse políticas y manuales de privacidad, un manual de capacitación, actualización y concientización del personal, un procedimiento de control interno, procedimientos ágiles, expeditos y gratuitos para recibir y responder dudas o quejas de los titulares; la creación de medidas y procedimientos técnicos que permitan mantener un historial de los datos personales durante su tratamiento; y *"constituir un mecanismo en el cual el responsable transmitente, le comunica al responsable receptor, las condiciones en las que el titular consintió la recolección, la transferencia y el tratamiento de sus datos" (Poder Ejecutivo de la República de Costa Rica, 2013)*[319].
- Determina los elementos por tomar en cuenta para el establecimiento y mantenimiento de las medidas de seguridad físicas, administrativas y lógicas para la protección de los datos personales; dentro de los que se encuentran la sensibilidad de los datos, el desarrollo tecnológico, las consecuencias de una posible vulneración, el número de titulares que pudieran verse afectados, las vulnerabilidades previamente experimentadas, el riesgo y otros factores aplicables.

[319] Punto que intenta fomentar el respeto a la cadena de control sobre la información personal.

- Obliga al responsable a informar al titular sobre irregularidades en el tratamiento o almacenamiento de sus datos y las opciones disponibles al titular con miras a solventar la situación u obtener más información.
- Afirma la capacidad de la agencia de verificar en cualquier momento el protocolo de actuación y su cumplimiento, para lo cual debe facilitarse a la agencia un *superusuario*, *"con perfil de consulta, aun cuando los datos estén siendo tratados por un encargado" (Poder Ejecutivo de la República de Costa Rica, 2013),* mediante el cual la agencia pueda consultar en cualquier momento y de oficio la base de datos[320].
- Se refiere a la transferencia de datos personales para lo cual se requiere no solamente la obtención del consentimiento informado, sino también el cumplimiento de los protocolos mínimos de actuación y la existencia, en el contrato de transferencia, de las mismas obligaciones para el responsable receptor que las existentes en el contrato firmado por el titular de los datos.
- Requiere la inscripción ante la Agencia de un número importante de elementos relativos a los datos tratados por los responsables, así como los protocolos mínimos de actuación, las medidas de seguridad adoptadas y demás factores relevantes.

[320] Punto sumamente discutido en tanto se considera que el término "superusuario" corresponde a un concepto mucho mayor que el reconocido por la ley. Esto podría facilitar el acceso y la modificación a los datos y sistemas de las empresas requeridas al punto de vulnerarlos o prestarse para abusos por parte de la Agencia. En este sentido debemos recordar que ni la ley ni el reglamento se han pronunciado sobre si dicho acceso debe darse de manera local o puede darse a distancia, por lo cual las preocupaciones de la industria se han visto acrecentadas conforme la Agencia comienza a aplicar el reglamento.

- Establece los aspectos procesales relativos a la protección de derechos ante la agencia, incluyendo tanto las causales como los requisitos de la denuncia, la admisibilidad, los medios de prueba y los procedimientos sancionatorios.
- Finalmente, define el Reglamento lo relativo a los cánones anuales de regulación, los procedimientos de cobro y otros elementos relativos al funcionamiento de la Agencia.

*Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones*

Dictado por ARESEP el 18 de marzo de 2010 y en vigencia en nuestro país desde abril de ese mismo año, el reglamento sobre el régimen de protección al usuario final procura *"establecer las normas técnicas, económicas, y jurídicas aplicables a las relaciones que con motivo de la prestación de los servicios de telecomunicaciones surjan entre los (operadores y proveedores) con sus clientes y usuarios, fijando las medidas técnicas y administrativas que permitan proteger los derechos y los intereses legítimos de los usuarios finales que utilizan servicios de telecomunicaciones" (Autoridad Reguladora de los Servicios Públicos, 2010).*

Con miras a lograr tal propósito, el Reglamento establece una serie de disposiciones técnicas a lo largo de sus catorce capítulos, dentro de las cuales es posible encontrar referencias a los procedimientos de reclamación por violación a la intimidad y derechos del usuario final; obligaciones de los operadores y proveedores; condiciones técnicas, legales y procedimentales de la prestación de los servicios de

telecomunicaciones; disposiciones relativas a los contratos de adhesión; facturación; disposiciones específicas para los servicios prepago; la declaración de derechos de los usuarios finales; las condiciones de instalación de los servicios de telecomunicaciones, las medidas de protección ante el fraude en servicios de telecomunicaciones; y finalmente los recursos, sanciones e infracciones existentes en cada caso.

Tal como podrá el lector apreciar a partir de la lectura de los temas antes mencionados, el Reglamento estudia una gran cantidad de elementos y por ello serán enfocados los artículos de este referidos a la protección de datos personales o a las condiciones en que deben prestarse los servicios convergentes de telecomunicaciones en nuestro país, a saber *(Autoridad Reguladora de los Servicios Públicos, 2010)*:

- Artículo 13: Detalla las obligaciones de los operadores y proveedores de conformidad con el articulado de la Ley Nº 8643 e incluye dentro de sus disposiciones la no discriminación en relación con sus obligaciones respecto a los derechos de los usuarios finales; acceso gratuito a servicios de emergencia, reporte de avería e interposición de denuncias; contar con centros de gestión capaces de informar al cliente sobre su consumo en el período de facturación; facilitar en todo caso los datos de contacto de la empresa; brindar información detallada, comparable, pertinente, fácilmente accesible y actualizada sobre sus servicios y su calidad e implementar los mecanismos para garantizar la exactitud y la confiabilidad de la facturación dictados por SUTEL.
- Artículo 14: Establece el deber de información existente entre los operadores y los proveedores con respecto a sus clientes, obligando a los primeros a suministrar información clara, veraz, suficiente y precisa relativa a las

condiciones específicas de prestación del servicio, niveles de calidad y tarifas, aún de manera previa al establecimiento del vínculo contractual.

- Artículo 18: Recuerda la posibilidad establecida por el artículo 6, inciso 8) de la Ley 8642, de que los operadores y proveedores brinden servicios convergentes cuando sus condiciones técnicas y legales se lo permitan, siempre y cuando cumplan con los estándares de calidad y las condiciones de prestación de los servicios establecidos por SUTEL.
- Artículo 21: Detalla el contenido necesario de los contratos de adhesión, el cual incluye desde características generales técnicas y legales, como los derechos de los usuarios y *"15) La información y los plazos referidos al tratamiento de los datos personales del cliente, en los términos exigidos por la legislación vigente en materia de protección de datos" (Autoridad Reguladora de los Servicios Públicos, 2010).*
- Artículo 29: Relativo al derecho del usuario a conservar su número telefónico (portabilidad numérica), el cual se torna relevante en tanto el número telefónico de un usuario debe, indudablemente, ser considerado como información capaz de identificarle (especialmente tras el uso continuado de este por parte del usuario) y de relacionar al individuo con la gigantesca cantidad de datos y metadatos almacenados por su operador o proveedor de servicios de telecomunicaciones.
- Artículo 43: Dicta el necesario registro de la información básica del cliente que contrata servicios en la modalidad prepago[321], lo cual debe incluir *"al menos,*

[321] Se debemos recordar al lector que en muchos países del orbe los servicios prepago no requieren de tal registro, sino que permiten comprar un número telefónico sin que exista ninguna manera directa de relacionar al cliente con el número. Esto conlleva varias ventajas desde el punto de vista de la protección de datos personales y en tanto es posible aquí un grado mucho mayor de anonimización del usuario final del servicio. A pesar de lo anterior, se debe también reconocer que la existencia de este

*pero sin limitarse: nombre, cédula de identidad vigente, documento equivalente o pasaporte a los extranjeros, dirección exacta, número telefónico de referencia o correo alternativo, y para personas jurídicas cédula jurídica, nombre o razón social, dirección física, correo electrónico y cualquier otra información que sea necesaria para localizar al cliente" (Autoridad Reguladora de los Servicios Públicos, 2010).*

- Artículo 44: Reconoce como derechos de los usuarios finales de telecomunicaciones *"los definidos en el artículo 45 de la ley 8642 y los demás establecidos en el ordenamiento vigente" (Autoridad Reguladora de los Servicios Públicos, 2010).*
- Artículo 46: Define las características y contenido del directorio telefónico del cual deberán formar parte todos los abonados de servicios de telefonía fija (y los de telefonía móvil previa autorización del abonado). De esta manera, deberán ser consignados en este registro el nombre, número telefónico y dirección exacta del abonado, los cuales deberán ser puestos a disposición del público por medio de las guías impresas y digitales facilitadas por los operadores.

  Finalmente, establece el artículo que: *"El operador o proveedor deberá excluir del directorio telefónico, los datos personales de los clientes que así lo soliciten ya sea en el momento de la suscripción del contrato o posteriormente, de manera oportuna. Esta exclusión no generará ningún cargo o costo adicional para el cliente" (Autoridad Reguladora de los Servicios Públicos, 2010).*
- Artículo 52: Establece la confidencialidad de los datos de los usuarios finales y la inviolabilidad de los servicios de telecomunicaciones con miras a "*evitar que*

registro en nuestro país responde a consideraciones de seguridad y conveniencia en la lucha contra el crimen.

*terceras personas puedan utilizar esta información para desarrollo de fraudes y/o acciones de usufructo ilegitimo; para tal efecto los operadores y proveedores se regirán por las disposiciones estipuladas en la Ley 8642, el reglamento sobre medidas de protección a la privacidad de las comunicaciones y demás establecidas en el ordenamiento jurídico vigente" (Autoridad Reguladora de los Servicios Públicos, 2010).*

- Artículo 53: Determina la necesaria verificación de la autenticidad de los datos aportados por el cliente al momento de subscribir el contrato de servicio.
- Artículo 57: Tipifica los fraudes en contra de los operadores o proveedores de servicio, reconociendo dentro de ellos la manipulación de la información por medio de un acceso no autorizado (sea local o remoto) a las plataformas de datos con la finalidad de borrar o alterar los registros existentes en ellas.
- Artículo 68: Tipifica el fraude de suplantación de identidad de equipos (*spoofing*[322]), y establece el deber de los operadores y proveedores de contar con sistemas de seguridad en sus redes que prevengan, restrinjan y bloqueen este tipo de fraudes.
- Artículo 75: En él se establece una serie de infracciones y se considera como falta grave, entre otras actividades *"d) no acatar las recomendaciones establecidas por la SUTEL para garantizar la confidencialidad de las comunicaciones en las redes de su responsabilidad; e) no hacer anónimos o eliminar los datos personales sobre el tráfico de los abonados cuando dicha información ya no sea necesaria para los efectos del establecimiento de las comunicaciones o su transmisión; f) no facilitar a los abonados medios sencillos para que puedan pronunciarse sobre la disposición de sus*

[322] El cual consiste en "sustituir un equipo o servidor que posee un servicio WEB al que accede el usuario, por otro equipo con el propósito de capturar su información privada, tales como pines o claves de acceso, datos personales e información bancaria, entre otros" (Autoridad Reguladora de los Servicios Públicos, 2010).

*datos en actividades comerciales; y g) no acatar lo solicitado por los suscriptores para publicar el detalle de datos que se publicarán en la Guía Telefónica" (Autoridad Reguladora de los Servicios Públicos, 2010).*

*Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones*

Dictado por el Presidente de la República junto con el Ministro de Ambiente, Energía y Telecomunicaciones, el Decreto Ejecutivo Nº 35205-MINAET, procura "*establecer las disposiciones reglamentarias sobre las medidas de protección a la privacidad y confidencialidad de las comunicaciones, derivadas del capítulo II del título II de la Ley General de Telecomunicaciones"* (Poder Ejecutivo de la República de Costa Rica, 2009).

El Reglamento establece, junto con la Ley Nº 8642 una serie de disposiciones en materia de privacidad y seguridad que serán aplicables a todos los operadores o proveedores de servicios que usen y exploten redes públicas de telecomunicaciones. Dichas disposiciones serán "*(…[323]) irrenunciables y de aplicación obligatoria sobre*

[323] Reza el artículo en cuestión que "Artículo 2º—**Ámbito de aplicación y alcance**. Están sometidos al presente reglamento todos los operadores o proveedores de servicios de telecomunicaciones que usen y exploten redes públicas de telecomunicaciones, independientemente del tipo de red. Los acuerdos entre operadores, lo estipulado en las concesiones, autorizaciones y en general, todos los contratos por servicios de telecomunicaciones que se suscriban de conformidad con esta Ley, tendrán en cuenta la debida protección de la privacidad y seguridad de las transacciones electrónicas que desarrollen los usuarios finales de los servicios de telecomunicaciones.
Las disposiciones que tutelen la privacidad de las comunicaciones establecidas en la Ley General de Telecomunicaciones y desarrolladas en este Reglamento son irrenunciables y de aplicación obligatoria sobre cualesquiera otras leyes, reglamentos, costumbres, prácticas, usos o estipulaciones contractuales en contrario" (Poder Ejecutivo de la República de Costa Rica, 2009).

*cualesquiera otras leyes, reglamentos, costumbres, prácticas, usos o estipulaciones contractuales en contrario"* (Poder Ejecutivo de la República de Costa Rica, 2009)[324].

Según su propio texto, el Reglamento reconoce los siguientes fines:

- Garantizar tanto el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos de carácter personal de abonados y usuarios.
- Promover que los proveedores y operadores adopten las medidas necesarias para garantizar la seguridad de sus servicios.
- Garantizar que la información divulgada tanto en guías de abonados como en recibos de servicios respete la confidencialidad y privacidad de los usuarios y no sea divulgada ni utilizada con fines comerciales.
- Asegurar los más rigurosos estándares de seguridad para los datos de tráfico y localización de los usuarios finales (así como su necesaria anonimización).
- Promover que la utilización de sistemas de venta directa no violente la intimidad de los usuarios.

Con miras a cumplir estos objetivos, el Reglamento dedica su segundo capítulo a la privacidad y confidencialidad de las comunicaciones, estableciendo una serie de obligaciones para los operadores y proveedores, a saber:

[324] Y, de acuerdo con el artículo tercero del reglamento, corresponderá a SUTEL garantizar el cumplimiento de las obligaciones de privacidad de las comunicaciones que se impongan a los operadores de redes de telecomunicaciones, para lo cual deberá este ente asegurar la adopción de medidas técnicas y administrativas por parte de los obligados dirigidas a garantizar tanto la seguridad en el almacenamiento y transferencia de las comunicaciones como la intimidad la las personas (Poder Ejecutivo de la República de Costa Rica, 2009).

- garantizar que las comunicaciones y sus datos de tráfico no sean escuchadas, grabadas, registradas, almacenadas, intervenidas o vigiladas por terceros sin consentimiento ni orden judicial.
- Adoptar las medidas técnicas y administrativas más avanzadas para dar cumplimiento a los principios de privacidad y confidencialidad e informar a SUTEL en cuanto conozca de riesgos en la seguridad de la red (e informar cuando este riesgo exceda las medidas que se encuentre obligado a tomar).
- Adoptar las medidas contractuales necesarias para asegurar que, dentro de sus relaciones contractuales, el personal que tenga acceso a datos sensibles respete los principios supramencionados (e igual disposición realiza con respecto a los funcionarios de SUTEL).
- Brindar los servicios de elaboración de guías de abonados y de consulta telefónica sobre números de abonado y cumplir al pie de la letra las disposiciones técnicas establecidas por el mismo reglamento al respecto, con el requerimiento del consentimiento informado de sus usuarios para incluir datos personales en las guías.
- Informar a sus abonados cuando sean brindados servicios de identificación de llamada y cumplir con las reglamentaciones técnicas relevantes a dichos servicios.
- Eliminar o anonimizar los datos de carácter personal sobre el tráfico y localización de los usuarios finales que hayan sido tratados y almacenados para establecer las comunicaciones. Asimismo, establece el deber de informar y solicitar el consentimiento informado del abonado con respecto al trato que se

le dará a sus datos personales; se debetambién facilitar un medio sencillo para retirar tal consentimiento.

- Eliminar o anonimizar los datos relativos al tráfico y la facturación de los usuarios en tanto no sean ya necesarios para los efectos de su transmisión, los cuales pueden ser utilizados solamente mediante el consentimiento informado del abonado para prestación de servicios con valor agregado o para la promoción comercial de servicios de telecomunicaciones.
- Conservar de manera confidencial los siguientes datos:

*"A. Datos necesarios para rastrear e identificar el origen de una comunicación:*

*1. Con respecto a la telefonía de red fija y a la telefonía móvil:*

*1.1) Número de teléfono de llamada.*

*1.2) Nombre y dirección del abonado o usuario registrado.*

*2. Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:*

*2.1) La identificación de usuario asignada.*

*2.2) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.*

*2.3) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.*

*B. Datos necesarios para identificar el destino de una comunicación:*

*1. Con respecto a la telefonía fija y a la telefonía móvil:*

*1.1) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios,*

*como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.*

*1.2) Los nombres y las direcciones de los abonados o usuarios registrados.*

*2. Con respecto al correo electrónico por Internet y la telefonía por Internet:*

*2.1) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.*

*2.2) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.*

*C. Datos necesarios para determinar la fecha, hora y duración de una comunicación:*

*1. Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.*

*2. Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:*

*2.1) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo de Internet (IP), ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.*

*2.2) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.*

*D. Datos necesarios para identificar el tipo de comunicación.*

*1. Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal,*

*conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).*

*2. Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.*

*E. Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considere ser el equipo de comunicación:*

*1. Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.*

*2. Con respecto a la telefonía móvil:*

*2.1) Los números de teléfono de origen y destino.*

*2.2) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.*

*2.3) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.*

*2.4) La IMSI de la parte que recibe la llamada.*

*2.5) La IMEI de la parte que recibe la llamada.*

*2.6) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.*

*3. Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:*

*3.1) El número de teléfono de origen en caso de acceso mediante marcado de números.*

*3.2) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.*

*F. Datos necesarios para identificar la localización del equipo de comunicación móvil:*

*1. La etiqueta de localización (identificador de celda) al inicio de la comunicación.*

*2. Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones"* (Poder Ejecutivo de la República de Costa Rica, 2009).

- Solamente tratar aquellos datos de localización distintos a los datos de tráfico tras ser estos anonimizados (o tras haber obtenido el consentimiento informado del usuario u orden judicial que lo ordene) con miras a brindar un servicio con valor agregado.
- Facilitar los datos de localización distintos a los datos de tráfico a la Comisión Coordinadora del Sistema de Emergencias 9-1-1 y a las instituciones que ella indique.

*Reglamento de Acceso Universal, Servicio Universal y Solidaridad*

Dictado por ARESEP el 16 de octubre de 2008, este reglamento se relaciona con la presente materia de estudio, únicamente en cuanto extiende expresamente el régimen de protección de la intimidad reconocido por la Ley General de

Telecomunicaciones a los beneficiarios del Fondo Nacional de Telecomunicaciones. Así, establece el artículo 28 de este reglamento que:

*"Trámite de quejas. De acuerdo con lo establecido en el Capítulo II de la Ley Nº 8642, el régimen de protección a la intimidad y derechos del usuario final también aplicarán a los beneficiarios de los proyectos de FONATEL. Los artículos 47 y 48 de la Ley Nº 8642, especifican los procedimientos necesarios para recibir, procesar y atender las quejas y denuncias sobre incumplimientos de los operadores que brindan servicios financiados por el FONATEL, en cuanto a calidad, precio y características de esos servicios" (Autoridad Reguladora de los Servicios Públicos, 2008).*

*Reglamento de Personas Refugiadas*

Promulgado por la Presidenta de la República y el Ministerio de Gobernación y Política el 28 de setiembre de 2011, el Decreto Ejecutivo Nº 36831-G es digno de mención en tanto establece, en su artículo octavo, el principio de confidencialidad con respecto al registro y tratamiento de la información de las personas en condición de refugio.

*"Artículo 8º Principio de Confidencialidad. La confidencialidad es el principio rector para el registro y manejo de la información de los solicitantes de la condición de refugiado y de las personas refugiadas declaradas.*

*Encuentra su fundamento en el derecho humano a la intimidad, reconocido en diversos instrumentos internacionales suscritos por Costa Rica, esencial para garantizar una protección internacional efectiva a las personas refugiadas. La falta de observancia de este principio, puede tener serias repercusiones en materia de protección y de seguridad a las personas*

*refugiadas y solicitantes, sus familiares y personas con las que se le pueda asociar, tanto en Costa Rica como en el país de origen"* (Poder Ejecutivo de la República de Costa Rica, 2011).

*Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor N° 7472*

Dirigido a hacer efectivas las disposiciones de la Ley Nº 7472, el Reglamento incluye en su artículo 224 disposiciones relativas a la publicidad de la información sobre los comerciantes y proveedores debidamente autorizados para la venta de los bienes y servicios sujetos a regulación (Ministerio de Economía, Industria y Comercio , 2013). Según el Reglamento, esta base de datos deberá ser puesta al servicio del público para brindar las certificaciones solicitadas, cumpliendo siempre con las disposiciones de la LGAP y de la Ley Nº 8968.

*Reglamento sobre el Registro Único de Personas Beneficiarias*

Dirigido a cumplir con los requisitos del artículo 96 de la Ley 8956, Ley Reguladora del Contrato de Seguros, el Reglamento asegura, bajo la garantía de confidencialidad de SUGESE, los datos financieros personales que constan en el Registro. A lo largo de su articulado, el Reglamento enumera los tipos de datos requeridos; establece las disposiciones relativas al acceso al registro; el esquema tarifario aplicable, y los

aspectos procesales de la solicitud de acceso a la información (Banco Central de Costa Rica, 2014).

### *Otra Normativa Relevante*

#### *Directriz del Ministerio de Justicia y Paz del 04 de abril de 2014*

Primera directriz oficialmente generada en la Agencia de Protección de Datos de los Habitantes, es titulada simplemente como "*Las personas físicas o jurídicas públicas o privadas propietarias o administradoras de bases de datos deberán adecuar sus procedimientos y reglas de actuación para cumplir con Ley Nº 8968 Protección de la Persona frente tratamiento datos personales"* (Ministerio de Justicia y Paz, 2014). Esta directriz comunica, en cinco breves artículos la obligación de adecuación y registro por parte de todos los interesados[325] y extiende, por tres meses el plazo otorgado por la ley[326].

#### *Resolución RCS-303-2012 SUTEL "Disposiciones complementarias, técnicas, económicas y administrativas para la implementación y operación del sistema integral de portabilidad numérica en Costa Rica"*

[325] Elemento indicativo de la falta de cumplimiento que ha caracterizado a la Ley hasta la fecha.
[326] Debiendo haberse registrado los entes e instituciones aludidos antes de concluir el día 05 de junio del 2014.

Dirigida a asegurar la correcta implementación de la portabilidad numérica en el país, esta resolución de la Superintendencia de Telecomunicaciones se caracteriza por requerir expresamente de todos los operadores de telecomunicaciones del país involucrados en dicho proceso deban cifrar *"todos los datos (números de teléfono, nombres, identificadores, y demás información) (…) con normas equivalentes o superiores a AES, utilizando un nivel de encriptación igual o superior a 256 bits. La ERPN (Entidad de Referencia de Portabilidad Numérica) debe garantizar que el cifrado de datos se utilice tanto en el contenido de las comunicaciones como en el almacenamiento de la base de datos"* (Superintendencia de Telecomunicaciones, 2012). Se constituye, de esta manera, en una de las pocas disposiciones normativas en mencionar expresamente un estándar internacional en relación con el cumplimiento de la Ley Nº 8968.

*Acuerdo 014-077-2012 SUTEL sobre Procedimiento de Comunicaciones no Solicitadas*

Generado en conformidad con las disposiciones de los artículos 3 inciso j), 41 y 42 de la Ley General de Telecomunicaciones, el artículo 4 inciso 1) del Reglamento Sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones y las disposiciones de la Ley Nº 8968, este acuerdo reconoce las disposiciones legales relacionadas con el proceso de respuesta ante las afectaciones al ámbito de intimidad de los usuarios finales, las cuales resume de la siguiente manera:

*"Los operadores de redes públicas y proveedores de servicios de telecomunicaciones, se encuentran habilitados, ante una eventual perturbación del ámbito de intimidad de un usuario final provocado por el envío de comunicaciones no solicitadas, para proceder con la suspensión*

*o desconexión del servicio, lo cual implica adicionalmente la adopción de medidas a nivel contractual respecto del cliente que remite dichas comunicaciones. 1) A solicitud de los usuarios finales, habilitar la restricción de tráfico entrante para un servicio telefónico específico o un conjunto de servicios (nacionales e internacionales). 2) A solicitud de la SUTEL, en casos debidamente motivados por violaciones a la intimidad, habilitar el bloqueo selectivo de un servicio telefónico o un conjunto de servicios telefónicos (nacional e internacional)" (Superintendencia de Telecomunicaciones, 2012)*[327].

Adicionalmente, el Acuerdo presenta cuatro posibles escenarios *"sobre los cuales deban tanto los operadores de redes públicas como los proveedores de servicios de telecomunicaciones, cumplir con diversas obligaciones legales y reglamentarias vinculadas con las promociones de venta directa y el tratamiento de las comunicaciones no solicitadas" (Superintendencia de Telecomunicaciones, 2012)*, a saber:

1) Incorporación de medidas técnicas y administrativas en los acuerdos e instrumentos contractuales (contratos de interconexión / contratos de adhesión).

   Escenario de gran relevancia al plantear, con base en las disposiciones del marco legal aplicable al sector telecomunicaciones, los únicos ejemplos conocidos a la fecha de cláusulas modelo relativas a la protección de la privacidad de los usuarios finales, las cuales son copiadas a continuación dada su innegable relevancia:

   - Cláusula aplicable para contratos entre los operadores y proveedores:

[327] Se debe resaltar en este punto el hecho de que el Acuerdo solamente haga mención a "servicios telefónicos" y no a servicios convergentes o a servicios de información, por lo cual no es clara la aplicabilidad de estas disposiciones en casos de abuso de tecnologías convergentes.

*"Las Partes implementarán los sistemas y las medidas técnicas y administrativas necesarias para garantizar el secreto de las comunicaciones, el derecho a la intimidad, la protección de los datos de carácter personal de los abonados y usuarios finales y preservar la seguridad de sus servicios.*

*Las Partes se comprometen a implementar las medidas técnicas y administrativas necesarias, tales como pero sin limitarse a bloqueos o desconexiones de servicios de conformidad con la normativa vigente, cuando tengan conocimiento por los medios definidos entre ambas, que uno de sus clientes se encuentra remitiendo comunicaciones no solicitadas a algún usuario final" (Superintendencia de Telecomunicaciones, 2012).*

- Cláusula aplicable para contratos de adhesión:

*"ENVÍO DE INFORMACIÓN PROMOCIONAL:*

*El cliente autoriza el envío de información promocional con fines de venta de venta directa, relacionada con los productos y servicios del (proveedor de servicio).*

*( ) SI ( ) NO*

*Indico el siguiente medio para recibir la información promocional:*

*( ) Correo Electrónico ( ) SMS ( ) Correo postal*

*( ) Otro medio_____." (Superintendencia de Telecomunicaciones, 2012)*

2) El operador o proveedor remite comunicaciones no solicitadas.

Escenario que plantea los pasos por seguir de parte del operador o el proveedor, el cual incluye recibir la denuncia; investigar internamente el origen de la comunicación; detener la comunicación mediante las medidas técnicas y organizativas necesarias; coordinar este proceso con otros operadores en caso de ser necesario; verificar ante SUTEL su cumplimiento y la apertura de un procedimiento administrativo en caso de continuarse dando el comportamiento.

3) El operador o proveedor recibe una reclamación de un usuario final que plantea la recepción de comunicaciones no solicitadas (ambos clientes tanto el emisor como el receptor son clientes de un mismo operador o proveedor "Tráfico *on-net"). *Según lo cual el operador o proveedor deberá: recibir la denuncia; verificar la situación y prevenir al usuario emisor de las penas aplicables; aplicar la restricción de tráfico entrante para el usuario receptor; y adoptar las medidas administrativas de corresponsalía internacional necesarias para solucionar situaciones en que estas comunicaciones provienen del extranjero[328], entre otras.
4) El operador o proveedor recibe una reclamación de un usuario final que plantea la recepción de comunicaciones no solicitadas (el operador que recibe la reclamación no es titular del servicio el emisor de la comunicación "Tráfico *of-net*"). Lo cual se asemeja en sus disposiciones y limitaciones a las encontradas en el escenario 3.

[328] Es precisamente en este momento que se torna relevante la limitación de las disposiciones del acuerdo a los servicios telefónicos en relación con los flujos transfronterizos de información y la problemática existente en materia de protección de datos personales, los cuales no son protegidos por el acuerdo en tanto constituyen servicios de información bajo la normativa nacional.

Finalmente, se debe de recalcar que si bien este acuerdo no se dirige a la regulación directa de las disposiciones técnicas relevantes sobre protección de datos personales, constituye un valioso ejemplo de las labores realizadas hasta la fecha por SUTEL, con miras a cumplir sus obligaciones como ente regulador del sector de telecomunicaciones.

*Decreto Ejecutivo Nº 46-H-MICITT sobre uso de soluciones de cómputo en la nube sobre otro tipo de arquitectura*

Decretado por la Presidenta de la República y los Ministros de Hacienda y Ciencia, Tecnología y Telecomunicaciones, el Decreto Ejecutivo Nº 46-H-MICITT se presenta como un intento por parte del Estado costarricense de *"implementar las Tecnologías de la Información y Comunicación bajo principio principios racionales de eficiencia en uso de recursos, efectividad en su aplicación a cada una de las áreas e interoperabilidad entre los diferentes sistemas con el objetivo de garantizar transparencia en la producción de datos, información y conocimiento referentes al quehacer estatal, adecuarse a las condiciones financieras del Estado, así como para propiciar incrementos sustantivos en la calidad del servicio brindado a los ciudadanos" (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2013).*

Para tal fin, el Decreto impulsa a todas las instituciones del sector público a adquirir (cuando sea posible y conveniente) soluciones de cómputo en la nube "ya sea para el usuario final o para el centro de datos propiamente, o cualquier otro tipo de desarrollo tecnológico". Asimismo, requiere el Decreto que sea realizada una evaluación técnica

que logre determinar que se obtiene la "misma calidad de servicio con computación en la nube como si se adquiriese la tecnología respectiva" y que para su implementación se insta a los jerarcas de los Supremos Poderes, así como de la totalidad de las instituciones Estatales[329].

[329] Este punto hace especial referencia a la Caja Costarricense del Seguro Social, lo cual abre la oportunidad para plantear una anotación contextual sobre la experiencia internacional sobre el tema.
La tendencia de impulsar la implementación de tecnologías en la nube no es nueva a nivel global, muchos otros países han optado por contratar servicios de computación en la nube para el manejo de las tareas de procesamiento y almacenamiento de la información con diversos niveles de éxito.
A pesar de ello, es necesario comprender que la computación en la nube (mal entendida por nuestra legislación como el simple acceso a las bases de datos a través de Internet) requiere de una arquitectura distribuida (lo cual le da el carácter difuso al cual hace referencia su nombre) que usualmente se encuentra regada a lo largo del mundo en gigantescos centros de datos en manos de empresas como Google y Microsoft.
La nube presenta una ventaja evidente sobre otras soluciones de computación pues, en tanto se renta de un proveedor de servicios privado el poder de procesamiento y capacidad de almacenamiento (redundante y distribuida) requerido, no se incurre en gastos innecesarios o excesivos como los relacionados con la construcción de un centro de datos que cumpla con los estándares de seguridad de la información.
El problema relacionado con este proceder se encuentra en tanto estos proveedores requieren asegurar la rentabilidad de su negocio, y para ello consideran múltiples factores que a menudo los llevan a ubicar sus centros de datos en países remotos (donde pueden, por ejemplo, contar con acceso a grandes cantidades de electricidad a precios reducidos o en los que no se verán afectados por legislación extensiva).
Evidentemente, esta situación por sí sola llama la atención a posibles problemas relacionados con la implementación masiva de la computación en la nube por parte de nuestro país. Pero aun cuando asumamos que el servicio es contratado a una empresa que posea buena reputación y que mantenga sus servidores en EEUU (por poner tan solo un ejemplo), o incluso en nuestro país, no debemos olvidar que se está confiando la estabilidad informática de la totalidad de los sistemas públicos a una empresa privada.
Esta situación podría parecer desdeñable al lector, sin embargo desde el punto de vista de la Protección de Datos Personales, la cesión de datos personales a empresas privadas ha sido históricamente caracterizada por traer consecuencias nada felices.
Encontramos un ejemplo de esta situación en el reciente escándalo sucedido en el Reino Unido, donde el Servicio Nacional de Salud decidió contratar servicios en la nube a la empresa transnacional Google, en cuyos servidores habrían de almacenarse y procesarse los registros de salud de miles de pacientes ingleses.
El surgimiento a la luz pública de esta concesión llamó inmediatamente la atención de los Comisionados Europeos de Protección de Datos y, por supuesto, de los ciudadanos, políticos y miembros de la prensa inglesa, quienes denunciaron la muy real posibilidad de abuso por parte de Google (y del gobierno Estadounidense, que recientemente reclamó jurisdicción sobre los servidores ubicados en el extranjero propiedad de empresas norteamericanas (Ax, 2014)) de esta información. (el lector puede encontrar más información sobre esta situación en (Ramesh, 2014).
A partir de las disposiciones del Decreto Nº 46-H-MICITT, las instituciones públicas costarricenses ahora deberán realizar consideraciones que incluyan también el amplio contexto que rodea a la computación en la nube. Por ello será necesario que dichas consideraciones sean tomadas con base en criterios sólidos que les permitan identificar los riesgos y los beneficios de la solución implementada y, por supuesto, que nuestro país cuente con una autoridad de protección de datos personales fuerte, estable

Finalmente, se debe resaltar que el Decreto contempla dentro de su octavo artículo la necesidad de que: *"La información que se capture en los instrumentos que se implementen y en cumplimiento de esta directriz, no deberá incluir detalles que pudieran comprometer la seguridad de la información y de la infraestructura tecnológica de las instituciones relacionadas. Asimismo, no debe arriesgar o comprometer información confidencial de los particulares a la que tuviera acceso la institución de que se trate" (Ministerio de Ciencia, Tecnología y Telecomunicaciones, 2013).*

*Documento N-2-2007-CO-DFOE "Normas técnicas para la gestión y el control de las Tecnologías de Información"*

Aprobado por la Contraloría General de la República en el 2007, este documento contiene un conjunto de políticas, normas y acciones para la gestión adecuada de recursos informáticos en el Estado, cuyo acatamiento no es solamente obligatorio según las disposiciones de la resolución R-CO-26-2007 de la Contraloría General de la República *"para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización"* (Contraloría General de la República, 2007, pág. 4); sino que obliga también a la administración a implementar sus disposiciones de manera efectiva y controlada dentro de dos años de su publicación.

El documento se encuentra dividido en cinco capítulos (Normas generales, planificación y organización, implementación de tecnologías de información, prestación de servicios y mantenimiento y seguimiento) que, en conjunto con su

y verdaderamente independiente que proteja los derechos individuales frente a las posibilidades abiertas por la pronta adopción masiva de tales tecnologías.

respectivo glosario, establecen los fundamentos técnicos y organizativos necesarios para asegurar el correcto manejo y control de los sistemas tecnológicos del Estado, de manera acorde con los principios de seguridad de la información.

Finalmente, se debe resaltar la relevancia de este documento al ser una importante guía para la seguridad de la información pública, cuyos preceptos *"prevalecerán sobre cualquier disposición en contrario que emita la Administración. Asimismo, que su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable"* (Contraloría General de la República, 2007, pág. 4).

*Política Judicial Dirigida al Mejoramiento del Acceso a la Justicia de las Niñas, Niños, y Adolescentes en Costa Rica*

Elaborada por la Comisión Nacional para el Mejoramiento de la Administración de Justicia y adoptada mediante Circular No.63 de 31 de mayo de 2011 del Poder Judicial, la Política Judicial Dirigida al Mejoramiento del Acceso a la Justicia de las Niñas, Niños y Adolescentes en Costa Rica, responde a los compromisos internacionales adoptados mediante la firma de las Reglas de Brasilia por parte de nuestro país e intenta apropiar sus principios en una revisión de los servicios de justicia.

Con miras a lograr estos objetivos, el Poder Judicial adopta una serie de decisiones relativas al efectivo acceso a la justicia y el respeto a los derechos de los menores de edad que intervienen en procesos judiciales. Entre estas decisiones, la Política incluye

lineamientos que comprometen al sistema judicial del país hacia la protección de la intimidad de las personas menores de edad.

Se puede ver plasmado este compromiso dentro del punto VI *Lineamientos estratégicos de la Política*, el cual afirma, en su punto d. lo siguiente:

*"Protección de los derechos de las personas menores de edad que intervienen en los procesos judiciales. Garantizar el pleno respeto al derecho al debido proceso de la persona menor de edad, el resguardo de su dignidad y la protección de la intimidad" (Poder Judicial de la República de Costa Rica, 2011).*

*Regulaciones en cuanto a la Transferencia de Información Personal de Clientes conforme Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales*

Emitidas por el Banco de Costa Rica de conformidad con los requisitos de la Ley Nº 8968, las Regulaciones señalan los tipos de información que el Banco podrá tratar, recopilar, almacenar, transferir[330] y ceder (puede el banco contratar a empresas que brinden tales servicios); así como de los derechos a disposición de los clientes respecto a la información en poder del Banco (Banco Nacional de Costa Rica, 2012).

[330] En este punto se debe señalar que las regulaciones no hacen mayores referencias a las transferencias transfronterizas de datos personales, sino que simplemente reserva un derecho genérico para transferir datos personales manteniendo siempre su responsabilidad ante el cliente.

*Directriz para Reducir la Revictimización de Niños, Niñas y Adolescentes en Condición de Discapacidad en Procesos Judiciales*

Dada mediante Circular 168 de 7 de diciembre de 2010, la Directriz para reducir la Revictimización de Niños, Niñas y Adolescentes en Condición de Discapacidad en Procesos Judiciales se dirige a los operadores y operadoras judiciales que conocen asuntos en los que intervienen personas menores de edad en condición de discapacidad y ordena mediante su directriz XX proteger la intimidad y privacidad de este sector humano que sufre usualmente situaciones de vulnerabilidad dentro de un proceso judicial.

*"XX. Derecho a la imagen. La autoridad judicial encargada deberá controlar que la dignidad del/a testigo o víctima en condición de discapacidad, no sea lesionada a través de publicaciones o cualquier exposición o reproducción de su imagen, o de cualquier otro dato personal que permita su identificación. Para ello podrá dictar medidas cautelares a favor del niño, niña o adolescente cuando su imagen, intimidad y privacidad sean lesionadas y ordenarle al PANI abrir proceso especial de protección en sede administrativa. Igualmente no se debe promover una imagen prejuiciosa por su discapacidad. Si se lesiona este derecho, es obligación del funcionario o funcionaria denunciarlo de conformidad con del artículo 47 del Código Civil"* (Poder Judicial de la República de Costa Rica, 2010).

*Código de Ética de las y los Profesionales en Comunicación*

Adoptado por el Colegio de Periodistas de Costa Rica como Reglamento No.158 de 16 de agosto de 2011, el Código de Ética de las y los Profesionales en Comunicación contempla en su artículo 24 la obligación de los profesionales de periodismo de *"conducirse de manera respetuosa en la obtención de las informaciones, con respeto al dolor ajeno, la privacidad y la intimidad" (Colegio de Periodistas de Costa Rica, 2011, pág. 24).* Asimismo, establece su artículo 38 la obligación de los profesionales de publicidad de *"Respetar el derecho a la privacidad e intimidad, así como la imagen de los sectores socialmente vulnerables, las personas físicas y jurídicas" (Colegio de Periodistas de Costa Rica, 2011, pág. 24).*

### *Síntesis de la Segunda Sección*

*A lo largo de la cual serán analizados los componentes que conforman el marco legal de las telecomunicaciones y la protección de datos en Costa Rica.*

Marco Regulatorio Vigente en Materia de Telecomunicaciones

El sistema legal aplicable para las telecomunicaciones se encuentra definido en nuestro país fundamentalmente por las siguientes normas:

- Tratados Internacionales
    - Convención Internacional de Telecomunicaciones: Ratificado en tres ocasiones, dirigido a preservar y ampliar la cooperación internacional para el mejoramiento y el empleo racional de las telecomunicaciones de todo tipo; introdujo oficialmente a Costa Rica ante la UIT.
    - Constitución y Convención de la Unión Internacional de las Telecomunicaciones: Extienden los fines de la UIT con base en una serie de objetivos adoptados por Costa Rica con dos reservas y declaraciones relevantes para la aplicabilidad de las recomendaciones de la UIT en el país.
    - Tratado Centroamericano de Telecomunicaciones y su Protocolo: Busca la construcción y uso conjunto de una red regional de telecomunicaciones.
    - Acuerdo Relacionado con la Organización Internacional de Telecomunicaciones por Satélite: Crea la OITS, estableciendo principios de no discriminación para las telecomunicaciones satelitales.
    - Convención Internacional de Telecomunicaciones Marítimas por Satélite: Crea la INMARSAT, con miras a perfeccionar las telecomunicaciones marítimas y aeronáuticas.
    - Tratado Centroamericano de Libre Comercio e Integración Económica: Procura fortalecer e integrar las economías de la región y mejorar los sistemas de telecomunicaciones.
    - Acuerdo Marco de Co-Operación con la Comunidad Económica Europea: Procura promover la cooperación regional mediante la investigación, el

intercambio de información, la formación de personal y la ejecución de proyectos de interés común.

- Declaración Conjunta entre los Gobiernos de Canadá y Costa Rica sobre Comercio Electrónico Global: Establece cinco principios compartidos dirigidos al fortalecimiento del comercio electrónico y de la infraestructura necesaria para tal fin, apoyando para ello a la UIT y la CITEL.
- Tratado de Libre Comercio entre Estados Unidos, Centroamérica y República Dominicana: Modifica radicalmente la realidad de las telecomunicaciones en Costa Rica y fundamenta el modelo actual seguido por el país en el tema.

- Normativa Nacional en Materia de Telecomunicaciones
  - Ley de Fortalecimiento y Modernización de las Entidades Públicas: altera el rol del ICE en el sector de telecomunicaciones a la vez que amplía y regula las competencias y atribuciones del MICITT en el área.
  - Reglamento al Título II de la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones: Refina las disposiciones necesarias para garantizar el nuevo rol del ICE de cara a la legislación administrativa del país.
  - Ley General de Telecomunicaciones: Se constituye como la nueva columna vertebral del sector telecomunicaciones, regulando un gran número de temas y asignando nuevas responsabilidades a los proveedores de servicios de telecomunicaciones (más no regula los servicios de información).
  - Reglamento a la Ley General de Telecomunicaciones: Procura cumplir con los objetivos de la LGT regulando con mayor claridad temas como el espectro radioeléctrico, las obligaciones de los operadores y los títulos habilitantes entre otros.
  - Ley de Creación del Sistema de Emergencias 911: De especial relevancia para el presente tema en tanto no solo crea el sistema 911, sino que

obliga a los operadores a facilitar a este los datos de localización del usuario que disponga el acceso al servicio.

- Ley de la Autoridad Reguladora de Servicios Públicos: Determina las facultades de ARESEP con respecto a SUTEL.

Marco Regulatorio Vigente en Materia de Protección de Datos Personales

- Normativa Internacional Vigente para la República de Costa Rica en Materia de Protección de Datos Personales
  - Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional: Hace referencia al tratamiento de la información relevante a casos de delincuencia organizada por parte de los Estados parte, estableciendo obligaciones entre estos. Aplicable solamente a delitos graves.
  - Convención Interamericana sobre Extradición: También relacionada con el tratamiento de los datos personales dentro de las solicitudes de extradición.
  - Declaración de La Antigua sobre Datos Personales: Crea la Red Iberoamericana de Protección de Datos, pero no constituye un instrumento de derecho positivo aprobado de manera alguna por la Asamblea Legislativa.
  - Estatuto de Roma de la Corte Penal Internacional: Incluye algunas disposiciones sobre protección de datos en relación con los elementos procesales por ella regulados.
  - Acuerdo de Cooperación Ambiental entre el Gobierno de Costa Rica y el Gobierno de Canadá: Constituye una muestra de la obligación de nuestro país de dar información dentro de una investigación transnacional.
  - Acuerdo Relativo a la Readmisión de Personas en Situación Irregular: Menciona expresamente la protección de datos, los cuales busca proteger según las legislaciones vigentes en cada Estado.

- Acuerdo de Diálogo Político y Cooperación: Contempla expresamente la cooperación en materia de protección de datos con base en las normas internacionales más estrictas.
- Acuerdo y Protocolo para el Intercambio de Información en Materia Tributaria con el Reino de los Países Bajos: Permite a las partes requerir y obtener información financiera y relativa a la propiedad de sociedades a la vez que el protocolo dispone de una serie de disposiciones dirigidas a proteger dicha información.
- Convención Internacional para la Protección de todas las Personas contra las Desapariciones Forzadas: Incluye disposiciones relevantes al acceso a la información.
- 100 Reglas de Brasilia sobre Acceso a la Justicia de las personas en Condición de Vulnerabilidad: Creadas como un conjunto de cien estándares básicos por seguir por parte de las más importantes redes del sistema judicial iberoamericano, a pesar de lo cual aún no han sido ratificadas.
- Reglas de Heredia sobre Difusión de Información Judicial: Constituyen un conjunto de estándares mínimos voluntarios que comprenden un conjunto de reglas, definiciones y alcances sobre protección de datos en los procesos judiciales.
- Protocolo Facultativo de la Convención sobre los Derechos del Niño Relativo a la Venta de Niños, la Prostitución Infantil y Utilización de Niños en la Pornografía: Procura la protección de los datos personales (intimidad e identidad) de los menores de edad víctimas.

- Normativa Nacional Relevante para la Protección de Datos Personales
  - Tratamiento Histórico Jurisprudencial de la Protección de Datos Personales en Costa Rica
    - Etapa de Reconocimiento Inconsciente: Caracterizada por ser reconocido el derecho a la autodeterminación informativa por la Sala Constitucional sin saber que lo está reconociendo, en defensa de otros derechos fundamentales.

- Etapa de Negación: En ella la Sala rechaza los recursos de amparo dirigidos a la protección de la autodeterminación informativa pues entiende que no se trata de materia protegible por medio de amparo constitucional.
- Etapa de Reconocimiento Casuístico: En ella vuelven a ser aceptados los amparos de protección a la autodeterminación informativa y se desarrollan casos concretos que generan el germen de la regulación plena.
- Etapa de Doctrina Jurisprudencial Genérica: En ella finalmente es reconocido efectivamente el derecho a la autodeterminación informativa por parte de la Sala Constitucional.
- Etapa de Doctrina Jurisprudencial Específica: Caracterizada porque la Sala Constitucional comienza a tratar temas específicos, ya no resueltos casuísticamente, sino sobre la base de la doctrina jurisprudencial ya asentada con anterioridad.
- Etapa de Remisión de Asuntos de Autodeterminación Informativa a la PRODHAB: En ella se da un distanciamiento cada vez mayor por parte de la Sala Constitucional del tema, en tanto considera que este debe ser atendido por PRODHAB.

- Leyes
  - Código Civil: Protege los derechos de la personalidad a lo largo del título segundo de su libro segundo.
  - Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales: Uno de los cuerpos normativos más relevantes en la actualidad sobre el tema para nuestro país, establece a lo largo de sus cinco capítulos las bases del sistema de protección de datos personales costarricense. Caracterizada, entre otros elementos, por limitar su protección a los datos de personas físicas.
  - Ley de Información No Divulgada: Busca proteger la información relacionada con los secretos comerciales e industriales de

personas físicas o jurídicas, por lo cual se encuentra tangencialmente relacionada con el tema en estudio.

- Código Penal: Comprende también un número de disposiciones relativas a los hechos punibles realizados en el extranjero y a otros delitos contra el ámbito de intimidad.
- Reforma de la Sección VIII, Delitos Informáticos y Conexos, del título VII del Código Penal: Reforma el Código Penal con tal de añadir una serie de delitos informáticos a este; caracterizado por comprender la información como bien jurídico tutelado y por extender su protección a las personas jurídicas.
- Ley Nº 9135: Reforma varios artículos del Código Penal en respuesta a los movimientos populares que tachaban a la Ley de Delitos Informáticos de ser una "ley mordaza".
- Ley contra la Delincuencia Organizada: Permite el combate activo de la delincuencia organizada mediante la creación de una plataforma de información policial, vinculada a los cuerpos policiales nacionales e internacionales.
- Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones: Asigna los fundamentos de estas actividades, con el requerimiento de una orden judicial para la procedencia legítima de estas y permite el empleo de todos los medios técnicos pertinentes para que tales actividades sean llevadas a cabo.
- Ley Constitutiva de la Caja Costarricense del Seguro Social: Reconoce tanto la necesidad de contar con bases de datos dirigidas al control y verificación del cumplimiento de las obligaciones con la seguridad social; como el carácter confidencial de esta información.
- Ley de Expediente Digital Único de Salud: Define las características y los principios que dirigirán el sistema de expediente digital por ser implementado en el país, a la vez que

reconoce elementos fundamentales de la protección de datos personales para este.

- Código Tributario: Incluye disposiciones específicas dirigidas a proteger el carácter confidencial de las informaciones tributarias obtenidas por la administración de los contribuyentes.
- Código de Comercio: Protege la información financiera individual al establecer la inviolabilidad de las cuentas corrientes bancarias.
- Ley Reguladora del Mercado de Valores: Regula el actuar de los participantes en el mercado de valores y salvaguarda la confidencialidad de su información, a la vez que regula el intercambio de información entre la SUGEVAL y sus homólogos internacionales.
- Ley Orgánica del Banco Central: Por medio de ella se dictan varias medidas relacionadas con la confidencialidad de la información de las entidades fiscalizadas por la SUGEF.
- Ley Reguladora del Contrato de Seguros: Contempla disposiciones expresas en materia de protección de datos personales en su artículo 21.

- Reglamentos
  - Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales: Añade disposiciones específicas en temas como el tratamiento de los datos personales y las medidas de seguridad, la transferencia de datos personales, el consentimiento, entre otros.
  - Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones: Dirigido al establecimiento de las normas técnicas, económicas, y jurídicas aplicables a la protección de los derechos e intereses legítimos de los usuarios finales de telecomunicaciones.
  - Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones: Establece una serie de derechos irrenunciables

y de aplicación obligatoria sobre cualesquiera otras leyes, reglamentos, costumbres, prácticas, usos o estipulaciones contractuales en materia de protección de la privacidad de los usuarios de telecomunicaciones.

- Reglamento de Acceso Universal, Servicio Universal y Solidaridad: En él se extienden los beneficios del régimen de protección a la intimidad y derechos del usuario final a los beneficiarios de FONATEL.
- Reglamento de Personas Refugiadas: En él se reconoce el principio de confidencialidad con respecto al registro y tratamiento de la información de las personas en condición de refugio.
- Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor: Por medio de él se requiere el establecimiento de una base de datos de comerciantes y proveedores de bienes y servicios regulados de acuerdo con lo dispuesto por la Ley Nº 8968.
- Reglamento sobre el Registro Único de Personas Beneficiarias: Reglamento dirigido a cumplir con las disposiciones de la ley Nº 8968 en relación con el registro y tutela de datos financieros personales.

- Otra Normativa Relacionada
  - Resolución RCS-303-2012 SUTEL: Establece la obligación de cifrar todos los datos personales relacionados con el proceso de implementación de la portabilidad numérica mediante un estándar equivalente o superior al estándar AES.
  - Procedimiento de Comunicaciones no Solicitadas: Reconoce el proceso de respuesta ante las afectaciones al ámbito de intimidad y establece cuatro procedimientos por seguir en cuatro posibles escenarios de comunicaciones no solicitadas; se establecen en el primero de ellos cláusulas modelo sobre

privacidad para contratos de interconexión y contratos de adhesión.

- Decreto Ejecutivo Nº46-H-MICITT sobre el uso de soluciones de cómputo en la nube sobre otro tipo de arquitectura: Por su medio el Ejecutivo promueve la adopción de soluciones en la nube por parte de todas las instituciones públicas, exhorta a los otros poderes a hacerlo y requiere que las soluciones no arriesguen o comprometan la información confidencial ni la seguridad de la información. Establece regulaciones en cuanto a la transferencia de información personal de clientes: aviso oficial del Banco Nacional de Costa Rica mediante el cual se notifica a sus clientes, de acuerdo con la Ley Nº 8968.
- Normas técnicas para la gestión y el control de las tecnologías de información: Es un conjunto de políticas, normas y acciones para la gestión adecuada de los recursos informáticos según los principios de seguridad de la información. Declarado de acatamiento obligatorio para el sector público.
- Regulaciones en cuanto a la transferencia de información personal de clientes: Aviso oficial del Banco Nacional de Costa Rica mediante el cual se notifica a sus clientes de acuerdo con la ley Nº 8968.
- Política Judicial Dirigida al Mejoramiento del Acceso a la Justicia de las Niñas, Niños, y Adolescentes en Costa Rica: Busca implementar las Reglas de Brasilia en el país, apropiando sus principios en una revisión de los servicios de justicia.
- Directriz para Reducir la Revictimización de Niños, Niñas y Adolescentes en Condición de Discapacidad en Procesos Judiciales: Busca dentro de sus postulados la protección del derecho a la imagen de los menores en condición de discapacidad.

- Código de Ética de las y los Profesionales en Comunicación: Obliga a los profesionales de periodismo a respetar el dolor ajeno, la privacidad y la intimidad.

## Capítulo II: Protección de Datos Personales en las Telecomunicaciones Convergentes, ¿una realidad en Costa Rica?

A lo largo de la presente investigación se ha podido de estudiar el marco teórico que rodea la protección de datos personales en la actualidad. A partir de un estudio amplio de la evolución histórica de la protección de la personalidad humana por un conjunto de derechos (humanos, fundamentales y de la personalidad), se posibilitó la introducción al estudio de cuatro derechos humanos que delimitan a la protección de datos personales en la actualidad (intimidad, privacidad, información y autodeterminación informativa).

A continuación fue realizado un análisis profundo sobre la protección de datos; rememorando el surgimiento de las tecnologías de la información y la comunicación y adoptando una perspectiva iusinformática se pudo explorar, a lo largo del capítulo segundo, las múltiples sutilezas que la definen y su relación con las telecomunicaciones convergentes, para finalmente exponer algunos de los mayores problemas creados en este contexto.

Un extenso tercer capítulo permitió examinar el contexto legal que caracteriza a la protección de datos en el plano internacional. Partiendo de dos sistemas regionales contrapuestos (europeo y estadounidense), pudieron comprenderse las diferencias entre un sistema de intensa regulación y uno de regulación mínima. El estudio de esta aparente incompatibilidad dirigió a examinar las soluciones adoptadas por los países que han seguido al habeas data y, finalmente, se han estudiado tanto los puntos

intermedios planteados por países que han creado legislación específica sobre protección de datos, como los múltiples sistemas existentes en el nivel internacional, que procuran solventar el problema causado por el carácter necesariamente transfronterizo de las telecomunicaciones modernas.

A lo largo del cuarto capítulo, se pudo examinar el contexto histórico, administrativo que rodea tanto al sector telecomunicaciones como la protección de datos en Costa Rica. Finalmente, se pudo estudiar el marco legal vigente en nuestro país para ambos temas, mediante una enumeración detallada de la normativa nacional e internacional relevante.

Una vez concluidas todas estas etapas, no puede más el autor que preguntarse ¿hasta qué punto es traducida en la realidad la protección de datos personales en Costa Rica? Y con miras a brindar una solución a esta interrogante, a continuación se realizará un análisis holístico del marco legal costarricense ya estudiado, en relación con la totalidad de los temas abarcados a lo largo de la presente investigación; esto para finalmente plantear, a lo largo de la segunda sección del presente capítulo, algunas recomendaciones dirigidas al mejoramiento de la situación de la protección de los datos personales frente a la convergencia de las telecomunicaciones en Costa Rica.

## Sección I: Análisis de la Protección de Datos en Costa Rica Frente al Derecho Comparado, ¿Cuenta Nuestro País con una Protección Adecuada?

Una vez concluida la exposición sobre el estado actual de los marcos normativos nacionales e internacionales que resultan relevantes para la protección de datos personales, se puede (y se debe) realizar un análisis crítico del estado actual de los sistemas implementados por nuestro país, con miras a determinar la adecuación de su protección a los estándares internacionales requeridos en un mundo inmerso en la convergencia de las telecomunicaciones.

A lo largo del siguiente análisis se habrán de recordar los procesos ya estudiados mediante los cuales la Comisión Europea determina si un país cuenta o no con un nivel adecuado de protección. Basados en el análisis de los factores regulatorios, instrumentales e institucionales y la realidad de la aplicación de la normativa existente[331], estos procesos contemplan también la adecuación de la normativa nacional a principios básicos y su inclusión de elementos adicionales que faciliten y garanticen la puesta en práctica de la normativa.

Asimismo, por medio de las siguientes páginas se examinarán algunos de los temas más importantes que han sido identificados en la presente investigación a la luz del derecho nacional e internacional. Específicamente, se enfocará la atención en los principios aplicables en materia de autodeterminación informativa y protección de datos en Costa Rica; el grado de protección brindado por nuestro país a los datos

[331] En este punto se debe aclarar que el análisis que a continuación presentaremos se verá limitado a los aspectos teóricos pues, no es posible contar a la fecha con datos claros sobre la aplicación real de la protección de datos personales en nuestro país.

personales; el nivel de adecuación de nuestra legislación con respecto a los estándares internacionales; y finalmente, la capacidad de reacción de Costa Rica frente a los retos planteados por la convergencia de las telecomunicaciones.

## Manifestación de los Principios y Derechos Relativos a la Autodeterminación Informativa y la Protección de Datos Personales en el Marco Normativo Costarricense

A lo largo de este primer punto se intentará identificar las diversas manifestaciones de los principios fundamentales de la protección de datos personales y el derecho de autodeterminación informativa en el marco normativo costarricense. La realización de este ejercicio permitirá contar con una perspectiva más profunda del tipo de normativa existente en nuestro país y la interrelación entre sus disposiciones dispersas. Asimismo, se logrará a partir de ello identificar aquellos vacíos, incompatibilidades o meras imperfecciones en los niveles más básicos de protección que brinda nuestro sistema, con miras a la aclaración futura de las técnicas y herramientas iusinformáticas de protección de datos personales aplicables en nuestro país[332].

Con miras a cumplir este objetivo, a continuación se reexaminarán brevemente los principios y deberes que a lo largo de esta investigación se han definido como fundamentales para el derecho de autodeterminación informativa y para las diversas etapas de la protección de datos personales, especificando en cada uno la ubicación y características de sus manifestaciones en la normativa nacional vigente.

[332] Asimismo, se debe recordar que el reconocimiento expreso de un principio por parte de un cuerpo normativo determinado procura reunir un conjunto de elementos capaces de dirigir el criterio judicial y administrativo en la aplicación de la normativa para todos aquellos casos que no se encuentren tutelados directamente por su articulado.
Frente a la importancia de estos elementos, la omisión de un principio determinado (o el que un principio no sea específicamente declarado como tal) por una ley dirigida a regular un tema como la protección de datos personales conlleva la posibilidad de que los derechos por ella tutelados sufran vulneraciones.

*Principios*

De acuerdo con lo estudiado a lo largo de los dos primeros capítulos de esta investigación, tanto el derecho de autodeterminación informativa como la protección de los datos personales se ven enmarcados por un conjunto de principios relativos a la calidad de los datos y al correcto accionar de los encargados del tratamiento.

Tal como se verá a continuación, estos principios no siempre corresponden con los vigentes en nuestro contexto[333], sino que han sido adoptados con diversos niveles de claridad por parte de la legislación costarricense de protección de datos personales, y han logrado manifestarse también dentro de las disposiciones positivas y jurisprudenciales que regulan las actividades del sector de las telecomunicaciones.

- Principio de Libre Circulación de la Información:

  Referido a la necesaria libertad de circulación de la información relacionada con el contexto global de las telecomunicaciones convergentes, este principio no se encuentra directamente contemplado por ninguna normativa nacional, a pesar de lo cual se encuentran referencias relevantes a este tema en:

  - Ley Nº 7593: En su artículo 78 asegura a las empresas de países con los que Costa Rica posea tratados internacionales vigentes el acceso a las redes y el uso de cualquier servicio de telecomunicaciones disponibles

[333] Esta afirmación puede ser verificada con tan solo examinar el articulado de la Ley Nº 8968 de Protección de la Persona Frente al Tratamiento Automatizado de sus Datos Personales, la cual afirma que la autodeterminación informativa abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en su segunda sección, la cual contempla únicamente dos principios (principio de consentimiento informado y principio de calidad de la información).

al público de manera transfronteriza, razonable y no discriminatoria, permitiéndoles, entre otras actividades: *"Suministrar servicios a los usuarios finales (…) realizar funciones de conmutación, señalización, procesamiento y conversión y usar protocolos de operación a su elección (y) Usar servicios de telecomunicaciones disponibles al público, para transmitir información contenida en bases de datos o almacenada en otra forma que sea legible por una maquina" (Asamblea Legislativa de la República de Costa Rica, 1996).*

- Ley Nº 4573: Pena en su artículo 196 la violación de correspondencia o comunicaciones y, en el artículo 196 bis la interferencia (entre otras conductas) con los datos de personas físicas o jurídicas almacenados en sistemas o redes informáticas o telemáticas.

- Principio de Restricción Legítima:

  Relacionado intensamente con el principio de legalidad que fundamenta el Estado de Derecho en nuestro país, este principio se encuentra plasmado a en múltiples locaciones de nuestro panorama legislativo.

  Partiendo del artículo 28 de nuestra Constitución Política, este principio ha sido analizado por nuestra Sala Constitucional quien lo comprende como *"un principio material que forma parte del régimen democrático, condición que le da un rango intrínsecamente fundamental (ver en este sentido, sentencias número 2002-01764 de las 14:37 horas del 20 de febrero del 2002 y número 2008-017305 de las 14:58 horas del 19 de noviembre del 2008, así como el voto 13.605-2009). El principio de reserva legal no sólo garantiza la libertad frente al resto de los ciudadanos, sino que*

*constituye una garantía de control frente al poder público (ver voto 1635-90)"* (Sala Constitucional de la Corte Suprema de Justicia, 2010)

Finalmente, dado nuestro contexto, se debe recordar que este principio puede verse planteado por el artículo 19 de la Ley General de la Administración Pública, el cual afirma que: *"1. El régimen jurídico de los derechos constitucionales estará reservado a la ley, sin perjuicio de los reglamentos ejecutivos correspondientes. 2. Quedan prohibidos los reglamentos autónomos en esta materia"* (Asamblea Legislativa de la República de Costa Rica, 1978).

- Principio de Apertura:

  Dirigido a reflejar la naturaleza transfronteriza de los flujos de datos, representa la disposición de la administración a permitir los nuevos desarrollos, avances, prácticas y políticas, sin obstaculizar estas en su rol de regulador de la protección de datos, sino incorporándolas dentro de su perspectiva.

  Si bien no ha sido contemplado expresamente dentro del marco regulatorio nacional[334], se puede afirmar que este guarda una fuerte relación con las disposiciones del artículo 27 de la Ley Nº 8642 en tanto este artículo permite expresamente a los operadores de redes y proveedores de servicios de telecomunicaciones, brindar nuevos servicios sin mayor trámite[335].

[334] Como punto aparte, debe resaltarse que este principio fue adoptado de manera clara y expresa por Brasil en su recientemente aprobado Marco Civil da Internet.

[335] Evidentemente, en nuestro contexto resultará más difícil asimilar el principio de apertura con las disposiciones del artículo supramencionado en tanto nos encontramos comparando no solamente un principio internacional, sino también dos marcos regulatorios diferentes: telecomunicaciones y protección de datos personales.
A pesar de lo anterior, un examen de la normativa nacional nos permite asegurar que, en buena teoría, este principio debería de cumplirse en Costa Rica aun cuando no se encuentre expresamente regulado.

- Principio de Pertinencia:

  Relacionado con la pertinencia, congruencia y proporcionalidad de los datos respecto al fin perseguido, este principio no ha sido previsto expresamente como tal por el marco legal relevante para el sector telecomunicaciones[336].

  A pesar de lo anterior, este principio ha sido citado por la jurisprudencia de nuestra Sala Constitucional, la cual declaró en su sentencia 8996-02 de las 10:38 horas del 13 de setiembre del 2002 que: *"Sólo podrán ser recolectados, almacenados y empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimos para que se han obtenido. (…) Los datos de carácter personal serán cancelados cuando hayan dejado de ser pertinentes o necesarios para la finalidad para la cual hubieren sido recibidos y registrados (…) Se prohíbe tener sobre una persona más datos que los necesarios a los fines del fichero"* (Sala Constitucional de la Corte Suprema de Justicia, 2004).

  Asimismo, es posible identificar algunas de sus manifestaciones en la normativa nacional, como por ejemplo[337]:

---

Según nuestra normativa, no es tarea de PRODHAB interponer trabas a la innovación (su interés primordial es el cumplimiento de la autodeterminación informativa) por lo que en el caso de los servicios de telecomunicaciones, estos podrán darse libremente en un marco de innovación constante una vez que cuenten con la respectiva concesión o autorización por parte de SUTEL siempre y cuando cumplan con las obligaciones relevantes en materia de protección de datos personales.

[336] Podríamos considerar tal vez que el primer párrafo del artículo 6 de la Ley Nº 8968 alude vagamente a este principio es aludido al afirmar que los datos deben ser adecuados, sin embargo no existe una mención específica a la necesidad de pertinencia, congruencia y proporcionalidad que define a este principio.

[337] Si bien en este punto incluimos únicamente manifestaciones positivas de este principio, debemos resaltar que existen también violaciones claras al mismo, como por ejemplo el que la Ley Nº 7425 permita la recolección indiscriminada e ilimitada de información a lo largo de su artículo noveno con base en el permiso otorgado por un juez en un proceso de investigación judicial.

- Ley Nº 8968: Es mencionado vagamente por su artículo 6 en su primer párrafo ("y adecuados") mas no se habla de la necesidad de congruencia y proporcionalidad de los datos con respecto al fin.
- Ley Nº 9162: Lo incluye dentro de las características claves de las soluciones tecnológicas implementadas al requerir que estas contemplen solo la información del paciente que corresponda.
- Reglamento sobre medidas de protección de la privacidad de las comunicaciones: Su artículo 30 afirma que solamente podrán ser tratados datos de localización distintos de los datos de tráfico *"en la medida y por el tiempo necesarios para la prestación de un servicio con valor agregado" (Autoridad Reguladora de los Servicios Públicos, 2010).*

- Principio de Finalidad:

  Procura la sujeción de los datos al fin original del procesamiento para el cual dio su consentimiento; este principio se encuentra plasmado por el inciso cuarto[338] del artículo sexto de nuestra Ley Nº 8968, el cual considera la "adecuación al fin" como uno de los cuatro elementos reconocidos por esta ley dentro de su principio de calidad de la información.

  Asimismo, este principio fue también recogido por la sentencia 04847-99 de nuestra Sala Constitucional, en la cual se afirmó que: *"Los datos de carácter*

[338] El cual reza lo siguiente: *"Los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley. Las bases de datos no pueden tener finalidades contrarias a las leyes ni a la moral pública"* (Asamblea Legislativa de la República de Costa Rica, 2011).

*personal objeto de tratamiento automatizado o manual no podrán utilizarse para finalidades distintas de aquellas para que los datos hubieren sido recogidos"* (Sala Constitucional de la Corte Suprema de Justicia, 2004).

Dentro de sus principales manifestaciones en el ámbito normativo nacional se encuentran:

- Ley Nº 8642: Su artículo 43 requiere la eliminación de aquellos datos de tráfico y localización tratados y almacenados bajo la responsabilidad de un operador o proveedor, que no sean necesarios para efectos de la transmisión de una comunicación o la prestación de un servicio.
- Ley Nº 8968: Incluye en el inciso cuarto de su artículo sexto el requisito de que: *"Los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines"* (Asamblea Legislativa de la República de Costa Rica, 2011).
- Leyes Nº 9048 y Nº 4573: Pueden relacionarse con este principio por medio de las disposiciones de su artículo 196 bis, el cual pena la desviación *"para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas" (Asamblea Legislativa de la República de Costa Rica, 2012).*
- Reglamento a la Ley Nº 8968: El artículo 4 b) requiere que el consentimiento obtenido se refiera a una o varias finalidades determinadas y definidas que justifiquen el tratamiento.

- Principio de Veracidad y Exactitud:

  Principio de gran importancia en tanto requiere que la información tratada responda fielmente a la realidad del interesado; este ha sido estudiado por la Sala Constitucional, la cual afirmó que: *"Si los datos de carácter personal registrados resultaren ser inexactos en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados, actualizados o complementados. Igualmente serán cancelados si no mediare un consentimiento legal y legítimo o estuviere prohibida su recolección"* (Sala Constitucional de la Corte Suprema de Justicia, 2004).

  Este principio ha sido manifestado también en el ámbito normativo nacional dentro de los siguientes instrumentos legales:

  - Ley Nº8968: Lo prevé expresamente a lo largo de los incisos 2 y 3 de su artículo sexto y requiere que los encargados de las bases de datos eliminen o modifiquen aquellos datos que falten a la verdad y les obliga también a tomar las medidas necesarias para *"que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados" (Asamblea Legislativa de la República de Costa Rica, 2011).*
  - Leyes Nº 9048 y Nº 4573: Penalizan por medio de su artículo 236 la difusión de información falsa a través de medios electrónicos, informáticos o mediante un sistema de telecomunicaciones capaz de afectar la seguridad y estabilidad del sistema financiero o de sus usuarios.

- Reglamento a la Ley Nº 8968: Lo contempla como parte de sus disposiciones sobre el derecho de autodeterminación informativa (artículo 12) y el derecho de rectificación (artículo 23).
- Reglamento de Medidas de Protección al Usuario Final de Telecomunicaciones: Puede ser relacionado con este principio dado el contenido tutelado por sus artículos 46 (contenido del directorio telefónico), 57 (fraudes en contra de los operadores o proveedores de servicio) y 58 (mensajes masivos).

- Principio de Lealtad:

  Relativo a la inexistencia de engaño o falsedad, este principio ha sido mencionado por la sentencia constitucional 8996-02, que prohíbe *"el acopio de datos por medios fraudulentos, desleales o ilícitos"* (Sala Constitucional de la Corte Suprema de Justicia, 2004). El principio de Lealtad fue contemplado indirectamente dentro del conjunto de principios observados por la Ley Nº 8968 en su artículo 5[339], por lo que se ve complementado por el Reglamento, el cual lo reafirma como requisito indispensable del consentimiento informado y afirma que la obtención del mismo debe ser "a) Libre: no debe mediar error, mala fe, violencia física o psicológica o dolo, que puedan afectar la manifestación de voluntad del titular" *(Poder Ejecutivo de la República de Costa Rica, 2013)*.

[339] "Se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos" (Asamblea Legislativa de la República de Costa Rica, 2011).

- Principio de Transparencia:

  Relacionado fundamentalmente con la apertura necesaria del encargado al escrutinio sobre el tratamiento de los datos personales que lleva a cabo, este principio no ha sido planteado como tal por nuestra legislación relevante[340], pero puede ser extrapolado a partir del deber de informar establecido por el artículo 5, inciso 1 y el derecho de acceso a la información establecido por el artículo 7 inciso 1[341] de la Ley Nº 8968 y las disposiciones de esta ley con respecto al rol de la PRODHAB en la verificación del cumplimiento de las obligaciones de seguridad y protección de datos.

  Este principio ha sido también reconocido por la normativa de telecomunicaciones relevante, específicamente por la Ley General de Telecomunicaciones en sus artículos 2 inciso h[342] y 3 inciso d[343] y puede extenderse dentro de este marco a la necesidad de transparencia en el tratamiento de datos personales por parte de los operadores, especialmente al

[340] A pesar de lo cual si ha sido reconocido expresamente por la Sala Constitucional, la cual afirma que "El derecho de autodeterminación informativa tiene como base los siguientes principios: el de transparencia sobre el tipo, dimensión o fines del procesamiento de los datos guardados" (Sala Constitucional de la Corte Suprema de Justicia, 2004).

[341] Específicamente con base en el punto d) de este artículo, el cual tutela el derecho a *"Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales"* (Asamblea Legislativa de la República de Costa Rica, 2011).

[342] "Incentivar la inversión en el sector de las telecomunicaciones, mediante un marco jurídico que contenga mecanismos que garanticen los principios de transparencia, no discriminación, equidad, seguridad jurídica y que no fomente el establecimiento de tributos" (Asamblea Legislativa de la República de Costa Rica, 2008).

[343] "Principios Rectores (…) d) Transparencia: establecimiento de condiciones adecuadas para que los operadores, proveedores y demás interesados puedan participar en el proceso de formación de las políticas sectoriales de telecomunicaciones y la adopción de los acuerdos y las resoluciones que las desarrollen y apliquen. También, implica poner a disposición del público en general: i) información relativa a los procedimientos para obtener los títulos habilitantes, ii) los acuerdos de acceso e interconexión, iii) los términos y las condiciones impuestas en todos los títulos habilitantes, que sean concedidos, iv) las obligaciones y demás procedimientos a los que se encuentran sometidos los operadores y proveedores, v) información general sobre precios y tarifas, y vi) información general sobre los requisitos y trámites para el acceso a los servicios de telecomunicaciones".

reunirse estas disposiciones con lo dispuesto por el artículo 7 inciso 1 d) supracitado.

- Principio de Información:

  Observado usualmente en conjunción con el principio de transparencia, el principio de información se manifiesta como una extensión del derecho del mismo nombre, que sustenta elementos básicos de la autodeterminación informativa (como por ejemplo el consentimiento informado). Es previsto por la sentencia No. 8996-02 como el primero de los principios básicos de la protección de datos.

  Adicionalmente, este principio se ha manifestado en otros elementos de nuestro marco legislativo, como lo son:

  - Ley Nº 8642: Protege el derecho de información en varias instancias, comprendiéndolo dentro de sus principios rectores (específicamente el de beneficio del usuario[344] y transparencia) y los derechos concedidos a los usuarios finales de telecomunicaciones.
  - Ley Nº 8968: Lo reconoce expresamente como uno de los principios básicos de la protección de datos en el país en el inciso primero de su Artículo 5.

[344] Ubicado en el artículo 3 inciso c) que reza "Beneficio del usuario: establecimiento de garantías y derechos a favor de los usuarios finales de los servicios de telecomunicaciones, de manera que puedan acceder y disfrutar, oportunamente, de servicios de calidad, a un precio asequible, recibir información detallada y veraz, ejercer su derecho a la libertad de elección y a un trato equitativo y no discriminatorio" (Asamblea Legislativa de la República de Costa Rica, 2008).

- Reglamento a la Ley 8968: Lo manifiesta por medio de sus artículos 4, 12, 21, 38 y 39.
- Reglamento de medidas de protección de la privacidad: Hace referencia expresa a este principio a lo largo de sus artículos 7, 9, 10, 12, 13, 18, 25, 26, 30 y 32.

- Principio de Confidencialidad:

  Relacionado con el deber de guardar secreto profesional y la no divulgación de la información tratada, este principio ha sido reconocido en el ámbito nacional por nuestra jurisprudencia constitucional, la cual afirma que: *"El responsable del fichero y quienes intervengan en cualquier fase del proceso de recolección y tratamiento de los datos de carácter personal están obligados al secreto profesional"* (Sala Constitucional de la Corte Suprema de Justicia, 2004). Más aún, se pueden encontrar referencias a este principio en la siguiente normativa:

  - Ley Nº 8660: Regula el manejo de información confidencial por parte del ICE en su artículo 35[345] y asigna al Consejo de la SUTEL el *"garantizar la privacidad y confidencialidad en las comunicaciones, de acuerdo con la Constitución Política" (Asamblea Legislativa de la República de Costa Rica, 2008).*
  - Ley Nº 7566: Lo reconoce en su artículo 12, el cual afirma que *"por las características de la información generada al operar el Sistema, los*

[345] "La información que el ICE y sus empresas obtengan de sus usuarios y clientes, será de carácter confidencial y solo podrá ser utilizada y compartida entre el ICE y sus empresas, para los fines del negocio. Su conocimiento por parte de terceros queda restringido, salvo cuando así lo solicite una autoridad legalmente competente, justificando su necesidad y por los medios respectivos" (Asamblea Legislativa de la República de Costa Rica, 2008).

*funcionarios de las instituciones involucradas deberán manejarla con la confidencialidad necesaria para salvaguardar la seguridad de los usuarios (Asamblea Legislativa de la República de Costa Rica, 1995).*

- Ley Nº 8968: Dedica la totalidad de su artículo 11 al deber de confidencialidad que recae sobre el responsable de la base de datos y quienes intervengan en cualquier fase del tratamiento de datos personales y extiende este deber no solamente al secreto profesional sino también al funcional.
- Reglamento a la Ley Nº 8968: Reafirma el deber de respeto a este principio por el encargado a lo largo de su artículo 31.
- Reglamento sobre medidas de protección de la privacidad de las comunicaciones: Sus artículos 1, 4 y 9 no solo lo afirman dentro de sus fines fundamentales, sino que también recuerdan el deber de SUTEL sobre la confidencialidad de las comunicaciones.
- Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones: Establece disposiciones relevantes a este principio en su artículo 6, en el cual se reconoce la inviolabilidad de las comunicaciones en el país, de conformidad con el artículo 41 de la Ley 8642 y asigna la responsabilidad de velar por la confidencialidad de estas a SUTEL.

- Principio de Seguridad de los Datos:

Relacionado con las medidas dirigidas a proteger la integridad y seguridad de la información tratada, este principio fue también recogido por la sentencia 2004-12239, en la cual nuestra Sala Constitucional cual afirmó como principio de la protección de datos que: *"**El responsable del fichero deberá adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado**, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que garanticen plenamente su seguridad e integridad y los de los centros de tratamientos, equipos, sistemas y programas"*[346] *(Sala Constitucional de la Corte Suprema de Justicia, 2004).*

En el caso del principio de seguridad de los datos, resulta interesante observar cómo la posición adoptada por la Sala Constitucional desde 1999 sentó un referente que ha sido replicado en buena cantidad de la normativa producida desde tal fecha. Así, en la mayor parte de los instrumentos legales analizados es posible encontrar la frase señalada en negrita como antecedente a disposiciones más específicas. Tal situación podrá ser observada en sus manifestaciones, encontradas fundamentalmente en la siguiente normativa relevante:

- Ley Nº 8642: Su artículo 42 recoge parte de la disposición antes mencionada para a continuación especificando que las medidas adoptadas deberán garantizar la seguridad de las redes y sus servicios.

[346] La negrita no es del original.

- Ley Nº 8968: En su artículo 10 reitera la disposición de la Sala Constitucional, agregando *"así como cualquier otra acción contraria a esta ley"* (Asamblea Legislativa de la República de Costa Rica, 2011).

  Además de esto, el artículo supracitado contempla la prohibición de registrar datos en bases de datos inseguras y aclara las medidas técnicas y organizativas especificando que: *"Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada" (Asamblea Legislativa de la República de Costa Rica, 2011).*

  Finalmente, debe señalarse que a pesar de incluir una sección entera de su articulado dirigida a la seguridad y confidencialidad del tratamiento de los datos, esta ley no enumera el principio de seguridad de los datos como uno de sus principios básicos.
- Ley Nº 9162: Ley que también copia a la Sala Constitucional en su artículo 11 para, a continuación reiterar las disposiciones de la Ley Nº 8968 sobre los mecanismos incluidos en las medidas adoptadas.
- Ley Nº 7593: En ella es asignada a SUTEL la responsabilidad de *"garantizar la seguridad de los mensajes" (Asamblea Legislativa de la República de Costa Rica, 1996)* recibidos de redes externas o extranjeras.
- Reglamento a la Ley Nº 8968: Dedica los artículos 27 a 39 a determinar el tratamiento de los datos personales y las medidas de seguridad aplicables en el país.

- Reglamento sobre medidas de protección de la privacidad de las comunicaciones: Afirma como uno de sus fines fundamentales la seguridad de los datos que deben ser protegidos mediante la adopción de los más altos estándares.

  Así, este reglamento dedica varios artículos[347] al tema, y asigna un importante papel a SUTEL en la seguridad de las telecomunicaciones (Artículo 3[348]); a la vez afirma que: *"Para tales efectos, los operadores o proveedores deberán considerar las técnicas más avanzadas a fin de garantizar un nivel de seguridad adecuado al riesgo existente" (Poder Ejecutivo de la República de Costa Rica, 2009).*

- Principio de Prohibición de Procesamiento de Datos a Beneficio de Inventario:

  Vagamente reconocido por los instrumentos positivos estudiados, este principio fue reconocido (hasta cierto punto) por nuestra Sala Constitucional desde 1999 al afirmar que: *"Se prohíbe tener sobre una persona más datos que los necesarios a los fines del fichero"* (Sala Constitucional de la Corte Suprema de Justicia, 2004). Asimismo, debe relacionarse este principio con el principio de finalidad examinado anteriormente, el cual, junto con el principio de consentimiento informado, sus manifestaciones en el plano nacional podrían brindar alguna protección ante este comportamiento.

[347] Específicamente los artículos 3, 4, 6 y 7.
[348] "La Superintendencia de Telecomunicaciones deberá asegurar la adopción de medidas técnicas y administrativas por parte de los operadores y proveedores para que se garantice la seguridad en el almacenamiento y transferencia de las comunicaciones como la intimidad de las personas" (Poder Ejecutivo de la República de Costa Rica, 2009).

- Principio de Aseguramiento Técnico:

  Relacionado fundamentalmente con la necesidad de contar con un ente capaz de asegurar técnicamente que los principios de protección de datos personales están siendo cumplidos. La principal manifestación de este principio puede ser encontrada en el artículo 12 de la Ley Nº 8968 y el artículo 33 del Reglamento de la Ley Nº 8968, los cuales reconocen la facultad de verificación del cumplimiento de los protocolos de seguridad que posee PRODHAB.

  En el caso costarricense este principio en particular cuenta también con un elemento adicional que reasegura la capacidad técnica de PRODHAB de determinar el cumplimiento de los encargados de las bases de datos de los principios aplicables. Este elemento puede encontrarse en las disposiciones de los artículos 44 y 45 del Reglamento a la Ley Nº 8968 que exigen a los encargados una cuenta *"un superusuario con perfil de consulta, aún cuando los datos estén siendo tratados por un encargado. (…) La Agencia podrá en cualquier momento y de oficio consultar dicha base de datos sin restricción alguna, cuando exista denuncia presentada ante la Agencia o se tenga evidencia de un mal manejo de la base de datos o sistema de información"* (Poder Ejecutivo de la República de Costa Rica, 2013).

- Principio de Licitud de los Criterios de Clasificación:

  Relacionado especialmente con la necesidad de que las bases de datos no realicen actividades ilegales (como por ejemplo tratar datos y metadatos para

determinar informaciones sensibles de los interesados), este principio se relaciona íntimamente con el principio de restricción legítima, el principio de responsabilidad y el principio de defensa de los datos especialmente protegidos. En nuestro país algunas de sus manifestaciones pueden encontrarse en las disposiciones de los artículos 5 (inciso 2)[349] y 6 (incisos 2 y 4)[350] de la Ley Nº 8968.

- Principio de Defensa de los Datos Especialmente Protegidos:

  Principio que dispone la necesidad de respeto a un grupo especial de principios cuyo tratamiento es considerado especialmente peligroso para los intereses del individuo; se encuentra retratado en el marco legal nacional en los siguientes instrumentos legales:

  - Ley Nº 7593: Como parte de su artículo 78 hace referencia a *"datos personales no públicos de los usuarios de servicios de telecomunicaciones disponibles al público"* (Asamblea Legislativa de la República de Costa Rica, 1996).
  - Ley Nº 8968: Que si bien no incluye expresamente este principio, sí brinda especial defensa a los datos sensibles dentro de la clasificación planteada por los artículos 3, 9 y 31.
  - Ley 4573: Su artículo 196 bis castiga con especial dureza *"c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la*

[349] Que prohíbe el acopio de datos por medios fraudulentos, desleales o ilícitos.
[350] Que asignan al responsable de la base de datos velar por que los datos sean tratados de manera leal y lícita" y requiere de este responsable eliminar tales datos en caso de que esté prohibida su recolección.

*salud, el origen racial, la preferencia o la vida sexual de una persona" (Asamblea Legislativa de la República de Costa Rica, 1970).*

- Ley 9162: Prohíbe, en su artículo 11, el tratamiento de toda la información contenida en el expediente digital único en tanto esta está constituida de datos sensibles.

- Principio de Consentimiento:

  Fundamento para la correcta recolección de información personal, el principio de consentimiento requiere la aceptación expresa e informada del sujeto de datos ante todo tratamiento[351] que se pretenda realizar a su información personal. Puede verse reflejado en las siguientes disposiciones normativas:

  - Ley Nº 8642: En la que es requerido el consentimiento informado como única excepción a la prohibición sobre el tratamiento de datos de tráfico y localización (artículo 43) y de comunicaciones no solicitadas (artículo 44).
  - Ley Nº 8968: Lo prevé como un principio fundamental de la protección de datos costarricense por medio de su artículo 5, en el cual se establece tanto la obligación de informar como los requisitos y excepciones para el consentimiento.
  - Leyes Nº 4573: Tal como se ha estudiado, nuestro Código Penal castiga severamente las violaciones de datos por medio de su artículo 196 bis,

[351] Como nota aparte se debe señalar que si bien este principio ha sido incorporado en una buena cantidad de leyes en nuestro país, a la fecha su aplicación en la práctica es sumamente limitada.

las cuales incluyen, por supuesto, el tratamiento sin consentimiento de los datos personales.

- Reglamento a la Ley Nº 8968: Dedica su capítulo II al consentimiento y aclara en él los requisitos del consentimiento (debe ser libre, específico, informado, expreso e individualizado).
- Reglamento sobre el régimen de protección al usuario final de los servicios de telecomunicaciones: Requiere del consentimiento de los interesados para incorporar la información de los usuarios de servicios móviles a los directorios telefónicos (artículo 46), y contempla la inexistencia del consentimiento como parte de sus disposiciones sobre fraudes y mensajes masivos (artículos 57 y 58).
- Reglamento sobre medidas de protección de la privacidad de las comunicaciones: Cuerpo normativo que incluye disposiciones relevantes al consentimiento como parte de sus artículos 6, 9-13, 25, 26, 30 y 31.

- Principio de Responsabilidad:

  De gran valor práctico (y que cada vez demuestra tener mayores aplicaciones en el nivel internacional por medio de una correcta aplicación contractual), este principio ha sido planteado claramente en una buena cantidad de la normativa nacional, que asigna al responsable de los sistemas el cumplimiento de las medidas necesarias para garantizar la tutela a los derechos de los usuarios.

  Algunos de los ejemplos más notorios de este principio pueden ser encontrados en:

- Ley Nº 8968: Asigna un amplio conjunto de responsabilidades al encargado (responsable) de las bases de datos a lo largo de sus artículos 3, 5, 6, 7, 10, 11 y 14.
- Reglamento a la Ley Nº 8968: En su artículo 6 establece expresamente disposiciones relativas a la carga de la prueba, la cual recaerá, para efectos de demostrar la obtención del consentimiento, en todos los casos en el responsable de la base de datos.

- Principio de publicidad:

  Principio relacionado con el deber de inscribir las bases de datos en un registro, es parte del conjunto de principios que no han sido reconocidos expresamente por la ley pero que a pesar de ello se encuentran tutelados por algunas de sus disposiciones. Específicamente, se pueden mencionar tres ejemplos de manifestaciones de este principio en el contexto nacional:

  - Ley Nº 8642: Requiere el registro de los operadores y proveedores de servicios (así como el registro de los servicios brindados por estos) en un Registro Nacional de Telecomunicaciones (Artículo 27).
  - Ley Nº 8968: Crea un registro de bases de datos reguladas, con coordinación de PRODHAB, a la vez que requiere el registro de todas las bases de datos con fines de distribución, difusión o comercialización (artículos 16 y 21).

- Reglamento a la Ley Nº 8968: Complementa las disposiciones supramencionadas por medio de sus artículos 44 a 57, los cuales definen el proceso de inscripción de las bases de datos ante la Agencia.

Lastimosamente, debe concluirse este punto señalando que no fue posible identificar manifestaciones del principio de separación de poderes informativos ni del principio de control del procesamiento, a lo largo del presente estudio de la normativa nacional. Esta situación se plantea como una extraña omisión dado que el panorama estudiado, a pesar de caracterizarse por no contemplar a los principios como tales, posee varias manifestaciones de estos.

*Derechos Subjetivos*

Elementales para la protección jurídica de los datos personales, los derechos subjetivos recogidos por el marco normativo costarricense poseen, como se estudió anteriormente, un carácter fundamentalmente reactivo[352], y fueron introducidos a nuestro derecho por vía de la jurisprudencia constitucional relacionada con las acciones de habeas data interpuestas a lo largo de la década pasada.

En la actualidad el derecho costarricense reconoce expresamente los derechos subjetivos de acceso a la información[353]; rectificación[354]; cancelación u omisión[355];

[352] Se debe recordar que estos derechos constituyen los fundamentos positivos del habeas data (visto por muchos años como única reacción posible bajo nuestro marco legal) y que responden también a una percepción de la protección de datos dirigida fundamentalmente hacia la reacción y la retribución ante los perjuicios sufridos por los sujetos interesados, y no hacia la prevención.
[353] Ley Nº 8968: artículo 7, Inciso 1; Reglamento a la ley Nº 8968: artículo 21.
[354] Ley Nº 8968: artículo 7, Inciso 2; Reglamento a la ley Nº 8968: artículo 23.

revocación[356] y al olvido[357]. Asimismo, se puede recalcar la existencia de medidas preventivas (principios) suficientes en nuestro marco legal, como para asegurar la existencia de un derecho a no sufrir perjuicios por el tratamiento de los datos personales[358].

Finalmente, también puede identificarse en nuestro país la vigencia del derecho de tutela especializada estudiado en los primeros capítulos de la presente investigación; sin embargo, debe recordarse que según las disposiciones de la Ley Nº 8968, este derecho tutelará única y exclusivamente a personas físicas[359].

### Técnicas y Herramientas de Protección de Datos en el Contexto Legal Costarricense

Partiendo de los sistemas estudiados en el título tercero de esta investigación; a continuación se presentan al lector algunas de las características fundamentales de las técnicas y herramientas comúnmente utilizadas en la protección de los datos personales. Siguiendo el estilo del examen hecho de los principios y derechos aplicables, se intentará complementar este listado con una breve referencia al reconocimiento que de ellas haya realizado la normativa nacional vigente.

---

[355] Ley Nº 8968: artículo 7, Inciso 2; Reglamento a la ley Nº 8968: artículo 25.
[356] Ley Nº 8968: artículo 5, inciso 2; Reglamento a la ley Nº 8968: artículos 7 a 10; Reglamento sobre medidas de protección de la privacidad de las comunicaciones: artículo 25.
[357] Reglamento a la ley Nº 8968: artículo 10; Ley Nº 8642.
[358] Específicamente gracias a las acciones preventivas existentes en el capítulo VII del Reglamento a la ley Nº 8968.
[359] En tanto las personas jurídicas no son reconocidas en nuestro país como sujetos de datos con capacidad para incoar procesos en la vía administrativa especializada (PRODHAB), únicamente pueden recurrir a la vía penal para defender de manera reactiva sus intereses).

*Técnicas de Seguridad de la Información*

Estudiadas a lo largo del segundo capítulo de la presente investigación, las técnicas de seguridad de la información se constituyen como parte fundamental de todo sistema de protección de datos personales, en tanto aseguran técnicamente la información personal en las diversas etapas del tratamiento de los datos.

Relacionadas con todas las capas de los sistemas de información, estas técnicas se basan en los principios fundamentales de confidencialidad, integridad y disponibilidad para generar políticas, normas y acciones capaces de asegurar la seguridad integral de la información mediante la adopción de una perspectiva holística en el planteamiento e implementación de estos sistemas.

La incorporación de las técnicas de seguridad de la información en el plano normativo, facilita la protección de los datos personales al plantear un conjunto mínimo de herramientas que deben ser implementadas en toda base de datos en el país. Tal como se estudiara en el punto anterior, algunas de estas técnicas han sido reconocidas en nuestro país por vía jurisprudencial, legislativa y reglamentaria; sin embargo, aún es posible encontrar vacíos importantes en su regulación e implementación.

Con miras a brindar al lector un mejor panorama del contexto actual de las herramientas relacionadas con la seguridad de la información, a continuación se mencionarán algunas de ellas, identificando su sustento normativo y realizando algunas observaciones sobre su implementación cuando sea necesario.

*Protocolos de Seguridad de la Información*

Dirigidos a detallar los procesos y procedimientos que garantizan la seguridad de la información, los protocolos de seguridad de la información contienen todas aquellas medidas técnicas y organizacionales que permitan prevenir y manejar los riesgos relacionados con las actividades realizadas por la organización[360].

Estos protocolos han sido regulados en el marco normativo costarricense fundamentalmente por medio del artículo 12 de la Ley Nº 8968 y los artículos 32, 33, 35 y 36 de su reglamento, los cuales los prevén como protocolos de actuación de emisión optativa por parte de los procesadores de datos personales en los que: *"establecerán los pasos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales, de conformidad con las reglas previstas en esta ley" (Asamblea Legislativa de la República de Costa Rica, 2011).*

Caracterizados por su necesaria inscripción ante PRODHAB y por extender al encargado del procesamiento una presunción "iuris tantum" del cumplimiento de las disposiciones de la Ley Nº 8968 relativa a la cesión de los datos personales, en nuestro país estos protocolos deben, por lo menos:

*"a) Elaborar políticas y manuales de privacidad obligatorios y exigibles al interior de la organización del responsable;*

*b) Poner en práctica un manual de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;*

[360] Así, es usualmente posible identificar dentro de estos protocolos disposiciones relativas a las responsabilidades y el comportamiento de todos los individuos encargados del sistema; las funciones de todos los interesados en el correcto funcionamiento del sistema; el plan de respuesta a incidentes; y los controles de seguridad (tanto físicos como digitales) relevantes. Lo anterior no significa que estos protocolos no puedan o deban incluir un número mayor de elementos, pues ello dependerá de las características de la información tratada y de la normativa aplicable en cada país.

*c) Establecer un procedimiento de control interno para el cumplimiento de las políticas de privacidad;*

*d) Instaurar procedimientos ágiles, expeditos y gratuitos para recibir y responder dudas y quejas de los titulares de los datos personales o sus representantes, así como para acceder, rectificar, modificar, bloquear o suprimir la información contenida en la base de datos y revocar su consentimiento.*

*e) Crear medidas y procedimientos técnicos que permitan mantener un historial de los datos personales durante su tratamiento.*

*f) Constituir un mecanismo en el cual el responsable transmitente, le comunica al responsable receptor, las condiciones en las que el titular consintió la recolección, la transferencia y el tratamiento de sus datos"* (Poder Ejecutivo de la República de Costa Rica, 2013).

*Registro de Incidencias*

Herramienta que permite el seguimiento histórico de las incidencias sufridas por la una empresa o institución en sus procesos, el registro de incidencias puede relacionarse con el historial del tratamiento de los datos personales requerido por el artículo 32 inciso e) del Reglamento a la Ley Nº 8968, así como con la bitácora que debe llevar PRODHAB según el artículo 45 de este reglamento.

Asimismo, este registro puede verse relacionado con las disposiciones establecidas por las normas técnicas para la gestión y el control de las tecnologías de información, las cuales reconocen en su punto 1.4.5 la necesidad de: *"establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI"* (Contraloría General de la República, 2007, pág. 4).

*Control de Acceso, Identificación y Autenticación*

Elementos fundamentales para la protección de la información frente a la posibilidad de que esta sea accesada, alterada, difundida o eliminada por personas no autorizadas; las medidas de control de acceso, identificación[361] y autenticación[362] deben encontrarse necesariamente en los protocolos de seguridad de la información y deben ser aplicados de manera cotidiana por la institución.

Curiosamente, este tema ha sido poco tratado por la normativa nacional, que usualmente se limita a requerir genéricamente la adopción de medidas técnicas y organizacionales necesarias[363]. Así, a la fecha únicamente se han podido encontrar disposiciones relevantes en la Ley Nº 8131[364] y en las normas técnicas para la gestión y el control de las tecnologías de información, las cuales establecen nueve requisitos por cumplir por parte de las instituciones públicas, en su punto 1.4.5; a saber:

a) *"Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.*
b) *Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.*
c) *Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.*

[361] Término que hace referencia al momento en que un usuario se da a conocer en un sistema de información.
[362] Término que hace referencia a la verificación realizada por el sistema a partir de la identificación del usuario.
[363] Respecto a este punto, nuestra Ley Nº 8968 establece siete factores para determinar las medidas de seguridad aplicables a los datos personales que trate o almacene en su artículo 35.
[364] Que menciona como delito informático el facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas en su artículo 111 inciso c).

d) *Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.*

e) *Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.*

f) *Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.*

g) *Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.*

h) *Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.*

i) *Manejar de manera restringida y controlada la información sobre la seguridad de las TI"* (Contraloría General de la República, 2007, pág. 4).

### *Gestión de Soportes y Documentos*

Elemento relacionado con el correcto manejo de los soportes (medios de almacenamiento de información) electrónicos y documentos de todo tipo que maneja la institución. Comprende usualmente la necesidad de que todo soporte identifique físicamente el tipo de información que contiene y, en caso de ser necesario por

tratarse de copias de seguridad, los datos relevantes de esta, con miras a asegurar su correcta ubicación en el inventario y posterior almacenamiento.

A la fecha, esta herramienta ha sido aludida únicamente por las normas técnicas para la gestión y el control de las tecnologías de información, las cuales afirman, en su punto 1.4.4 el deber de las organizaciones de: *"establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios (Contraloría General de la República, 2007, pág. 4).*

*Herramientas de Control de Transferencias*

Elemento fundamental para la protección de todos los tipos de información, las técnicas de seguridad de la información deben comprender también las herramientas dirigidas a solventar la ineludible vulnerabilidad que enfrenta la información transmitida a través de todo tipo de redes informáticas, causada por la infraestructura misma de la red[365] .

En el contexto legal de la protección de datos costarricense, estas han sido vagamente establecidas por el artículo 34 del reglamento a la Ley Nº 8968, el cual requiere que: *"el responsable deberá velar porque el encargado de la base de datos y el intermediario tecnológico cumplan con dichas medidas de seguridad, para el resguardo de la información" (Poder Ejecutivo de la República de Costa Rica, 2013).*

[365] Debe recordarse en este punto que el carácter distribuido y descentralizado de las redes de telecomunicaciones basadas en la conmutación de paquetes hace imposible la determinación a priori del camino que seguirán los paquetes de datos (ni el número de intermediarios que los redirigirán hasta llegar a su destino).

Adicionalmente, puede encontrarse una mención más específica de los mecanismos por implementar en el artículo 1.4.4 inciso a) de las normas técnicas para la gestión y el control de las tecnologías de información, el cual requiere *"implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información" (Contraloría General de la República, 2007).*

*Procesos de Actualización*

Dado el carácter siempre cambiante del panorama tecnológico que rodea a las técnicas de seguridad de la información, a nadie debería sorprender que la necesidad de contar con medidas siempre actualizadas se encuentre contemplada por estas. Tal como lo establece su nombre, este elemento procura el establecimiento de métodos organizados y planificados de actualización de las medidas con miras a evitar imprevistos o desperfectos que puedan poner en riesgo la seguridad del sistema.

En Costa Rica esta previsión ha sido contemplada también por el Reglamento a la Ley Nº 8968, el cual establece, en su artículo 37 que: *"Los responsables deberán actualizar las medidas de seguridad cuando ocurran los siguientes eventos:*

a) *Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable;*
b) *Se produzcan modificaciones sustanciales en el tratamiento o almacenamiento, que deriven en un cambio del nivel de riesgo;*
c) *Se modifique la plataforma tecnológica;*

*d) Se vulneren los sistemas de tratamiento o almacenamiento de datos personales, de conformidad con lo dispuesto en la Ley y el presente Reglamento; o,*

*e) Exista una afectación a los datos personales, distinta a las anteriores.*

*En el caso de datos personales sensibles, cuando la ley lo permita, el responsable deberá revisar y, en su caso, actualizar las medidas de seguridad correspondientes, al menos una vez al año"* (Poder Ejecutivo de la República de Costa Rica, 2013).

### *Contratos y Cláusulas Modelo de Protección de Datos*

Dirigidas a extender y facilitar la implementación de la protección de datos personales en el ámbito nacional, la creación y publicación de contratos y cláusulas modelo, es un servicio brindado usualmente por las autoridades reguladoras de protección de datos que responde a sus objetivos de educación y extensión.

Común especialmente en el ámbito europeo, esta práctica responde a la necesaria adopción de todas aquellas medidas que garanticen el correcto cumplimiento de las disposiciones legales para la protección de datos por parte de los sujetos privados. Así, los contratos y cláusulas modelos se presentan a los encargados de una base de datos como una valiosa herramienta que puede ser incorporada gratuita y fácilmente en sus contratos.

La redacción de contratos y cláusulas modelo se constituye entonces en una responsabilidad fundamental por ser cumplida por parte de los entes reguladores

nacionales[366], que aumenta la seguridad de la información personal a lo largo de sus posibles cesiones y transferencias transfronterizas. En este sentido, la incorporación expresa de esta obligación por parte de los instrumentos normativos relevantes resulta conveniente en tanto legitima los documentos generados en el plano nacional e internacional.

A pesar de que la normativa costarricense sobre protección de datos no hace referencia expresa a la necesidad de generar cláusulas y contratos modelo, o a su adopción por parte de los encargados de las bases de datos, a lo largo de este estudio ya se han identificado algunas disposiciones relevantes al tema; a saber:

- Ley Nº 8968: Atribuye a la PRODHAB, en su artículo 16, los deberes de velar por el cumplimiento de la normativa en materia de protección de datos por personas y entes públicos y privados (inciso a); promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de datos (inciso h); y, finalmente, de dictar las directrices relevantes necesarias de ser implementadas por las instituciones públicas (inciso i).

  Adicionalmente, esta ley requiere también en su artículo 22 que PRODHAB promueva *"entre las personas y empresas que recolecten, almacenen o manipulen datos personales, la adopción de prácticas y protocolos de actuación acordes con la protección de dicha información" (Asamblea Legislativa de la República de Costa Rica, 2011).*
- Ley Nº 8642: Establece en su artículo 41 que: *"Los acuerdos entre operadores, lo estipulado en las concesiones, autorizaciones y, en general, todos los contratos por*

[366] O, en el caso europeo, por la Comisión Europea, apoyada por el grupo de comisionados nacionales de protección de datos (Grupo de Trabajo Artículo 29).

*servicios de telecomunicaciones que se suscriban de conformidad con esta Ley, tendrán en cuenta la debida protección de la privacidad y los derechos e intereses de los usuarios finales"* (Asamblea Legislativa de la República de Costa Rica, 2008).

Asimismo, resulta relevante a este tema el artículo 46 de esta ley, en el cual se asigna a SUTEL la tarea de homologar "*los contratos de adhesión entre proveedores y abonados, con la finalidad de corregir cláusulas o contenidos contractuales abusivos o que ignoren, eliminen o menoscaben los derechos de los abonados"* (Asamblea Legislativa de la República de Costa Rica, 2008).

- Acuerdo de SUTEL sobre procedimiento de comunicaciones no solicitadas: Recomienda la incorporación de dos cláusulas modelo de privacidad en los contratos (de adhesión y entre operadores y proveedores de servicios) de telecomunicaciones[367].

### *Buenas Prácticas Corporativas*

Elemento de gran importancia para la adopción masiva de mayores estándares de protección, las buenas prácticas de manejo de la información son resultado usualmente de acuerdos generados entre los diversos sectores corporativos, por medio de los cuales logran implementar comúnmente un conjunto de disposiciones capaces de proteger tanto sus intereses como los de sus usuarios.

[367] Las cuales pueden ser examinadas por el lector en el apartado dedicado a este acuerdo en el capítulo anterior.

En el ámbito costarricense, esta solución ha sido prevista por el artículo 22 de la Ley 8968, el cual asigna a PRODHAB la tarea de promover la adopción de "prácticas y protocolos de actuación acordes"*(Asamblea Legislativa de la República de Costa Rica, 2011)*.

### *Autorregulación Vinculante*

Solución normativa adoptada fundamentalmente dentro del sistema de regulación mínima encontrado en Estados Unidos. La autorregulación vinculante promueve la adopción de compromisos normativos y técnicos por parte de las empresas encargadas del tratamiento de datos personales, los cuales se tornan vinculantes mediante su registro ante el ente regulador, por lo que su incumplimiento puede ser penalizado según el régimen sancionatorio aplicable.

A pesar de adquirir cada vez mayor popularidad en el plano internacional, estas medidas no han sido previstas por el marco normativo costarricense, por lo que aún cuando una compañía decida adoptar medidas de protección de datos mayores a las requeridas por la Ley, un eventual incumplimiento no podría ser sancionado por PRODHAB[368].

### *Privacidad por Diseño*

[368] Salvo que este haya sido previsto expresamente por la Ley Nº 8968.

Las técnicas y principios de privacidad por diseño constituyen en la actualidad uno de los mayores logros en la protección real de los datos personales. Contempladas, entre otros, por los marcos normativos europeos, la privacidad por diseño tutela la privacidad y la autodeterminación informativa, por medio de su incorporación en todas las etapas de los procesos implementados por entes públicos y privados.

Lastimosamente, el estudio realizado de la normativa relevante a las telecomunicaciones y la protección de datos, pone en evidencia una completa omisión de referencias a la privacidad por diseño en el plano nacional. Estas omisiones se presentan como extrañas, dada la reciente promulgación de la normativa nacional sobre la materia y, especialmente, considerando la existencia de variadas iniciativas internacionales que han reconocido su importancia[369].

### *Ombudsman Corporativo/Institucional para la Protección de Datos Personales*

Incluido usualmente dentro de las disposiciones normativas de protección de datos, este punto hace referencia a la necesidad de contar con un ente fiscalizador imparcial e independiente dentro de toda institución o ente que maneje datos personales. Mediante la aplicación de los principios de seguridad de los datos, aseguramiento técnico y responsabilidad, la figura del *ombudsman* se puede entender en este contexto como una herramienta que une los intereses públicos y privados que deben dirigir la buena gobernanza de los datos personales en la actualidad.

[369] Como por ejemplo las resoluciones y declaraciones de las Conferencias Internacionales de Autoridades de Protección de Datos, en las cuales nuestro país ha participado en el pasado reciente.

Encargado de examinar continuamente los procesos realizados por su institución, el *ombudsman* labora en pro del cumplimiento de las disposiciones de protección de datos vigentes y la protección de los intereses de los titulares de los datos. Su rol dentro de las instituciones se relaciona tanto con el control interno, como el servir de nexo con las agencias de protección de datos nacionales (e internacionales, de tratarse de una corporación transnacional).

La figura del *ombudsman* de datos no ha sido contemplada directamente por la legislación nacional, y si bien es cierto que en la actualidad PRODHAB promueve la incorporación de la figura dentro de los entes fiscalizadores de las instituciones públicas[370], no será posible asegurar un nivel adecuado de protección de los habitantes si dicha figura no es también adoptada masivamente por las empresas privadas encargadas del tratamiento de datos personales.

### *Convenios Interinstitucionales*

Herramienta de indispensable aplicación para asegurar la protección de los datos personales en los diversos mercados regulados; la creación de convenios interinstitucionales que vinculen al ente regulador nacional con instituciones públicas y privadas, facilita las labores de extensión y colaboración que asuma PRODHAB.

En nuestro país, solamente se pueden encontrar vagas referencias a estas herramientas en el artículo 22 de la Ley Nº 8968[371], por lo que no es posible afirmar

[370] (Artavia Chavarría, 2014).
[371] El cual requiere la coordinación de estrategias de comunicación y divulgación con los gobiernos locales y la Defensoría de los Habitantes de la República.

que la Agencia (o cualquier otra institución pública relacionada con el tema) se encuentre efectivamente requerida a formar este tipo de alianzas[372].

### *Referencias a Estándares Internacionales y Protocolos Técnicos*

Tal como se afirmó en la sección dedicada al tema, la adopción de sistemas interoperables y actualizados requiere la coordinación técnica y jurídica de las soluciones por aplicarse en el nivel nacional. Para ello, el ente regulador debe ser capaz de determinar de manera clara y ágil las normas de seguridad y protección de datos por ser implementadas por parte de los proveedores de servicios y encargados del tratamiento de datos personales en el país.

En el plano nacional, la aplicación de estas herramientas en el sector de telecomunicaciones costarricense depende de la correcta comunicación entre PRODHAB y SUTEL, instituciones que adoptan roles diversos según las disposiciones relevantes encontradas en las leyes Nº 8660 y Nº 8698.

Tal como recordará el lector, la Ley Nº 8660 asigna a SUTEL (en sus artículos 2 y 60) la potestad de dictar las disposiciones técnicas relevantes para todos los actores del sector telecomunicaciones y de verificar el cumplimiento de estas[373].

Por otro lado, el artículo 16 (incisos a), h) e i) de la Ley Nº 8968 asigna a PRODHAB la responsabilidad de dictar las directrices necesarias para la implementación de

[372] A pesar de esta situación, según la Directora Nacional de PRODHAB, para mayo de 2014 la agencia ha logrado formalizar ya algunos de los primeros instrumentos de entendimiento interinstitucionales y procura fortalecer estas iniciativas en el futuro.
[373] Asignándose a SUTEL el asegurar el cumplimiento de las medidas de privacidad aplicables al sector telecomunicaciones.

procedimientos adecuados en instituciones públicas[374]; el promover y contribuir en la redacción de normativa relacionada con el tema; y velar por el cumplimiento de la legislación aplicable a la protección de datos personales.

De esta manera, el marco normativo actual limita el papel de PRODHAB a la fiscalización del cumplimiento de la normativa de protección de datos[375], a la vez que le asigna la tarea de apoyar a SUTEL en la elección de los métodos técnicos[376] de protección de datos y de seguridad de la información aplicables[377]. Frente a este panorama, corresponde a PRODHAB realizar un seguimiento y acercamiento institucional que asegure el cumplimiento de sus deberes y objetivos[378].

### Capacidad de reacción frente a la convergencia de las telecomunicaciones

Una vez concluido el estudio de las herramientas de la protección de datos personales reconocidas por el marco legal costarricense, procede a examinar la capacidad de adaptación del sistema de protección de datos personales aplicado en nuestro país de

[374] Asimismo, debemos resaltar que una lectura del artículo 16 no permite determinar satisfactoriamente la capacidad de PRODHAB de dictar directrices vinculantes para el sector privado en general.
[375] Tarea que es también asignada a SUTEL.
[376] Los cuales deberán responder a los principios rectores del sector telecomunicaciones, siendo el más importante de ellos el principio de neutralidad tecnológica.
[377] La Resolución RCS-303-2012 nos presenta con uno de los principales precedentes en la determinación de estándares técnicos para la protección de datos personales por parte de SUTEL. Tal como lo especificamos en la sección relevante, el punto XVIII de dicha resolución requiere que *"A fin de cumplir con la Ley N° 8968, Ley de Protección de la Persona Frente al Tratamiento de sus datos personas, todos los datos (números de teléfono, nombres, identificadores, y demás información) deberán ser cifrados con normas equivalentes o superiores a AES, utilizando un nivel de encriptación igual o superior a 256 bits"* (Superintendencia de Telecomunicaciones, 2012).
[378] Deber que aún debe ser cumplido, pues a la fecha ni las máximas autoridades de SUTEL (Méndez, Marín, & Steller, 2013) ni de PRODHAB (Artavia Chavarría, 2014) han coordinado ningún tipo de acercamiento interinstitucional.

cara al conjunto de problemas generados por la convergencia de las telecomunicaciones.

Para tal fin, a continuación se retomarán los cinco problemas señalados en los puntos finales del segundo capítulo, contextualizándolos y exponiendo su relación con el marco normativo ya examinado.

### *Proliferación de Cookies*

#### *Un Breve Experimento: Detección de la Información Obtenida por Medio de Cookies en el Caso Costarricense*

Tal como podrá imaginar el lector, la problemática que rodea a las *cookies* no es ajena al ámbito costarricense. Según RACSA, Costa Rica cuenta actualmente con un nivel de penetración de Internet de un 43.1%, con más de dos millones de usuarios conectados a la red (Miniwatts Marketing Group, 2011). Lastimosamente, este nivel de inclusión digital no se ha visto acompañado en nuestro país por una correcta educación técnica de los usuarios finales, por lo que el uso indiscriminado de métodos de rastreo no ha sido percibido aún por la mayoría de la población como una amenaza.

Lastimosamente, a la fecha nuestro país no cuenta con un estudio oficial relacionado con el uso de tecnologías de rastreo y captura de datos transaccionales. Ante esta perspectiva, a continuación se presentan al lector los resultados de una investigación experimental que relacionada con los datos liberados por un usuario costarricense en su paso por el Internet. Para ello, se procurará emular los resultados que obtendría un

usuario cualquiera, que navegue por la red sin conocer el peligro representado por las cookies y que no tome medidas especiales para controlar su uso.

- Metodología:

El experimento tuvo lugar desde el día veintiséis de septiembre del año 2011 hasta el día veintiséis de mayo del año dos mil trece, en la casa de habitación del suscrito investigador. Mediante el uso de la herramienta *Collusion*[379] desarrollada por Mozilla Inc. se realizó un rastreo de las páginas web visitadas, así como de aquellas páginas de terceros que eran informadas del paso del investigador por el internet y que inyectaron cookies en su computadora.

A partir de la fecha de inicio del experimento y hasta el final de este, se dio un uso normal del sistema informático, accediendo a tantas páginas web como resultara necesario, por un estimado de tres horas diarias. El investigador no realizó cambio alguno en su computadora ni adoptó ninguna medida especial dirigida a evitar ser rastreado.

- Análisis de Datos:

La herramienta utilizada facilitó al investigador una salida principal de datos y una secundaria. La salida principal de datos se encuentra conformada por un gráfico interactivo, el cual se encuentra conformado por un fondo negro inicialmente vacío, al cual son agregadas en tiempo real las páginas visitadas por el usuario (círculos azules) y las páginas de terceros (círculos grises) que eran notificadas de su paso por dichas

[379] Actualmente conocida como Lightbeam (Mozilla Inc., 2014).

páginas. Collusion identifica por medio de líneas grises que interconectan dichos puntos las relaciones existentes entre las diversas páginas.

El gráfico facilitado por la herramienta tiene en su formato original carácter dinámico, por lo cual refleja mediante un cambio en el tamaño de los círculos correspondientes la cantidad de conexiones contextuales existentes entre las páginas. A mayor tamaño de un círculo, mayor cantidad de páginas le han enviado información sobre el usuario. Asimismo, la herramienta permite acercarse o alejarse (hacer zoom, o modificar la perspectiva) al gráfico con miras a obtener mayor detalle.

A partir de la figura 3, las imágenes obtenidas muestran el gráfico dinámico en el máximo nivel de alejamiento permitido por la herramienta Collusion, por lo que debe realizarse la aclaración inicial de que la herramienta muestra en este nivel las páginas web más importantes y aumenta el tamaño del círculo de cada página según esta se relacione con un número mayor de páginas. Asimismo, resulta necesario recordar que la herramienta permite observar con mayor acercamiento las diversas páginas, con miras a identificar la totalidad de páginas visitadas.

La salida secundaria de datos consiste en un informe escrito del contenido de dicho gráfico, en el cual se establece la dirección de la página web; si la página fue o no visitada por el usuario; el número de visitas realizadas; el nombre de la página que refiere o de la que proviene la información del usuario, y el tipo de datos transferidos durante la visita a la página en cuestión.

- Resultados:

Dado el carácter dinámico e interactivo del gráfico proporcionado por la herramienta utilizada, los resultados de la principal salida de datos fueron capturados mediante la toma de una imagen estática. La primera captura fue realizada cinco minutos después de instalada la aplicación, tiempo en el cual fueron visitadas como prueba base diez páginas web; el gráfico resultante es el siguiente:

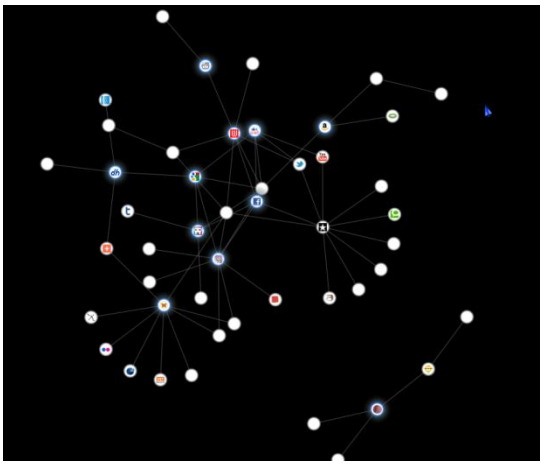


Figura 1: Imagen tomada el 26 de noviembre de 2011 a las 18 horas con 24 minutos

(Disponible en mayor definición en el Anexo 5)

En el primer gráfico son observables diez puntos azules correspondientes a las diez páginas web visitadas, así como treinta y siete páginas web que fueron alertadas del paso del investigador por la red, dado que las páginas visitadas no solamente instalan sus propias cookies, sino que también instalan cookies de terceros para realizar diversas funciones (tales como proveer video, experiencias sociales o publicidad personalizada al usuario).

En este primer gráfico se pueden observar con claridad las relaciones existentes entre las páginas de terceros y las páginas principales, las cuales conforman un tejido un poco denso, pero todavía descifrable. Tal situación varió considerablemente para el

final del primer día del experimento, momento en el cual el gráfico tenía el siguiente aspecto:

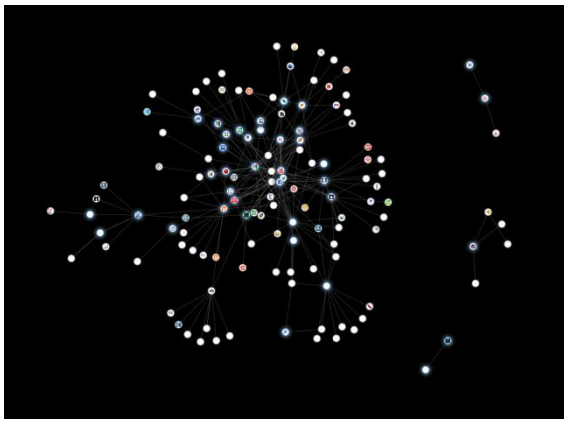


Figura 2: Imagen tomada el 26 noviembre de 2011 a las 23 horas con 30 minutos

(Disponible en mayor resolución en el Anexo 6)

En la figura 2 se puede observar cómo cinco horas después de haber iniciado el experimento en cuestión, habían sido visitadas ya treinta y nueve páginas por el usuario en su paso usual por el internet. Sin embargo, el incremento en el número de páginas visitadas causó una explosión en el número de páginas que habían instalado cookies en la computadora del usuario; este subió a más de noventa.

Asimismo, es posible observar cómo las páginas web comienzan a unirse en pequeños núcleos dependiendo de sus relaciones (siendo las páginas más cercanas al centro las que comparten mayor cantidad de cookies de terceras partes, lo cual a su vez permite el rastreo continuo del comportamiento del usuario a través de diversos sitios por medio de la agregación de datos).

Concluido el primer día de uso de la herramienta, esta continuó funcionando automáticamente, y no fue sino alrededor de un año más tarde que se realizó el

siguiente muestreo. En tal fecha, para sorpresa del investigador, el gráfico obtenido había crecido en complejidad y tamaño y no fue posible tomar una fotografía completa de él sin antes alejar la perspectiva al máximo. El gráfico correspondiente a un año de uso de Internet es el siguiente:

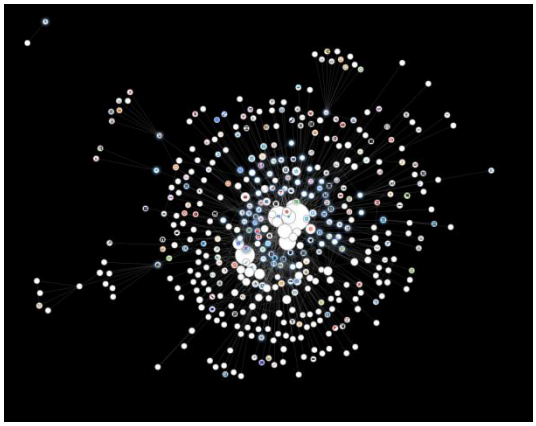


Figura 3: Imagen tomada el 8 de noviembre de 2012 a la 1 hora con 23 minutos

(Disponible en mayor resolución en el Anexo 7)

La figura 3 permite observar con mayor detalle cómo a lo largo del año transcurrido, la cantidad de páginas accesadas por el investigador se había estabilizado, por lo que la herramienta solamente mostraba en su mayor nivel de alejamiento las páginas accesadas con mayor regularidad. Asimismo, para la fecha el número de páginas de terceros que instalaron cookies en el sistema causaron el crecimiento de la cantidad de relaciones existentes entre ellas, tal como lo muestra el crecimiento en el tamaño de los círculos centrales.

El experimento fue concluido al cumplirse los veinte meses de haber iniciado. Para esta fecha, el gráfico poseía la siguiente apariencia:

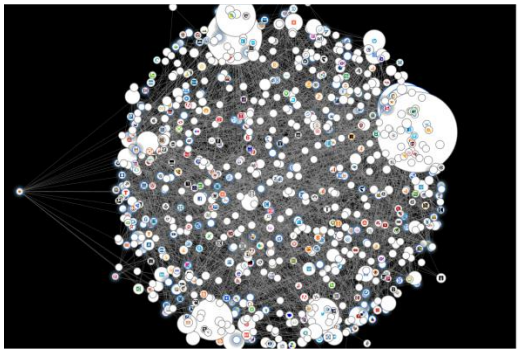


Figura 4: Imagen tomada el 26 de Julio de 2013 a las 22 horas con minutos

(Disponible en mayor resolución en el Anexo 8)

En la Figura 4 puede observarse un impresionante aumento en la interrelación de las páginas web, así como un aumento considerable en el número de círculos cuyo tamaño había aumentado por contar con un mayor número de conexiones.

Para esta fecha es posible identificar por lo menos 125 páginas web visitadas con relativa frecuencia por el usuario (por lo que pueden ser identificadas a simple vista dentro del gráfico), y un mínimo de 620 páginas importantes pertenecientes a terceros que rastreaban el paso del usuario por la red por medio de cookies. Finalmente, es necesario recalcar la evidente existencia de infinidad de líneas que representan las interrelaciones existentes entre las páginas web visitadas y las páginas de terceros.

Finalmente, debe señalarse que con respecto a la salida secundaria de datos, esta indica que en total fueron recibidas y almacenadas dentro de la computadora del investigador un mínimo de 1135 cookies; se visitaron durante estos veinte meses por lo menos 2696 páginas ".com", 175 páginas ".info", 96 páginas ".org", 49 páginas ".cr", y 11 páginas ".info".

- Conclusiones:

A lo largo de los veinte meses de duración del experimento, fue posible observar un incremento constante en la cantidad de cookies almacenadas, el cual se correspondió con el incremento en el historial de páginas visitadas. Asimismo fue observado un incremento exponencial en las líneas que identificaban las interrelaciones entre las páginas visitadas y las páginas de terceros.

Evidentemente, el presente experimento no pretende demostrar ningún tipo de correlación estadística entre las páginas visitadas y el número de cookies a las que se expone; sin embargo, permite observar de manera gráfica y simple realmente la extensión del problema encontrado.

Las imágenes tomadas de la salida gráfica de la herramienta Collusion permiten identificar el peligro ante el cual se encuentra cualquier usuario costarricense de Internet en la actualidad, dada la inevitable captura de información personal que sufrirá a manos de páginas web de terceros, sin darse cuenta siquiera de ello.

Por otro lado, los resultados de la salida escrita del programa permiten ratificar los resultados evidenciados en la salida gráfica y afirmar que alrededor de la mitad de las páginas visitadas en la actualidad requieren del uso de cookies para su funcionamiento.

### *Las cookies y el marco normativo costarricense*

A pesar de la gran importancia de las cookies en el funcionamiento del internet y del alto riesgo demostrado en el apartado anterior, el análisis realizado de la normativa

nacional relevante permite observar la inexistencia de disposiciones normativas relacionadas con el uso de cookies u otras tecnologías similares en nuestro país (en tanto estas son utilizadas fundamentalmente por los operadores de servicios de información y no por operadores de servicios de telecomunicaciones). Por ello, el planteamiento de reformas normativas capaces de llenar estas lagunas debe ser considerado prioritario en nuestro país.

Tal como lo ha sido establecido anteriormente, el sistema costarricense de protección de datos personales contempla algunos de los elementos necesarios para fundamentar eventualmente directrices o futura legislación dirigida a asegurar la protección del individuo frente a estas técnicas. Así, una interpretación amplia de los principios planteados por el artículo 5 de la Ley Nº 8968[380] de PRODHAB, podría brindar al regulador o al legislador con fundamento suficiente como para plantear algunas limitaciones básicas[381] al uso de estas tecnologías en nuestro país.

A pesar de tan imperiosa necesidad, es necesario que todo esfuerzo normativo que busque brindar soluciones al problema, realice un estudio más detallado de las técnicas y procesos que se pretende regular. El legislador debe recordar que las cookies y las técnicas de rastreo cumplen un papel fundamental en el funcionamiento del internet y por ello no pueden ser simplemente prohibidas o limitadas innecesariamente, sino que deberán ser objeto de una regulación uniforme, razonada

[380] Y específicamente la referencia a *"otros medios para la recolección de datos personales" (Asamblea Legislativa de la República de Costa Rica, 2011)* encontrada en el inciso 1 del artículo supracitado.
[381] Lamentablemente, aun cuando sea posible imaginar un abordaje a la regulación de estas técnicas por medio de directrices o reglamentos creados específicamente con tal fin, tal proceder podría verse afectado seriamente por el limitado ámbito de aplicación establecido por el artículo 2 de la ley Nº 8968.

y claramente delimitada, que cumpla con los estándares de interoperabilidad que para tal fin sean generados en el plano internacional.

### *Elaboración de Perfiles y Redes Sociales*

Tal como se estudió a lo largo del cuarto capítulo de la presente investigación, Costa Rica cuenta con uno de los mayores índices de penetración de internet en la región, el cual se ha visto acompañado de un surgimiento notable de los usuarios de Internet móvil[382]. Esta situación se ha visto aparejada a un importante incremento en el número de usuarios de redes sociales en nuestro país, quienes cada día más las utilizan para ejercer sus derechos de información, libre expresión, comunicación y participación ciudadana.

Este incremento en el conjunto de tecnologías disponibles a los usuarios costarricenses ha acarreado también problemas para la autodeterminación informativa, relacionados con el uso de redes sociales. Actualmente la elaboración de perfiles por parte de los usuarios y la publicación indiscriminada de información personal es un problema que la sociedad costarricense comparte con el resto del mundo; esta problemática se ve manifestada en nuestro contexto en los más diversos ámbitos[383].

[382] Tecnología que como afirmamos anteriormente ha logrado popularizar el acceso a Internet y disminuir notablemente la brecha digital gracias a que facilita sus servicios de manera ubicua y por precios mucho inferiores a otros medios de conexión a la red.

[383] Siendo comunes en el contexto nacional los casos de individuos que han sufrido afectaciones por un mal manejo de su presencia en las diversas redes sociales. Específicamente nos referimos a todos aquellos casos en que usuarios de redes sociales han incurrido en prácticas irresponsables y han sufrido por ello consecuencias laborales, sociales, emocionales, políticas y otros.

Más aún, el creciente nivel de interconexión experimentado por los usuarios costarricenses de redes de nueva generación, implica que ellos se enfrentan día tras día con el surgimiento de nuevas tecnologías y métodos dirigidos a canalizar toda la información generada por ellos hacia fines oscuros, sin su consentimiento.[384]

De esta manera, actualmente el contexto nacional de la protección de datos personales se ve confrontado con un conjunto de herramientas y tecnologías dirigidas a agregar datos personales que, al igual que las redes sociales sobre las cuales se basan, son alimentadas por los usuarios mismos en su lucha por simplificar el manejo de las diversas manifestaciones de su personalidad virtual (perfiles, avatares y otras formas de identificación digital).

Popularizadas en los últimos años, estas herramientas se presentan hoy en diversas modalidades y mientras que algunas continúan sirviendo únicamente a las grandes corporaciones o Estados por medio de sofisticados sistemas de espionaje, comúnmente se presentan en formas mucho más mundanas.

Efectivamente, aún sin saberlo, un número cada vez mayor de usuarios costarricenses utilizan y alimentan día tras día estos "*agregadores de redes sociales*"[385], los cuales se han visto incorporados poco a poco dentro de los sistemas operativos de sus dispositivos móviles al punto de que actualmente resulta difícil (por no decir

[384] Se hace referencia en este punto, por poner un ejemplo, a los *agregadores de redes sociales*, herramientas dirigidas a unificar la totalidad de los datos producidos por el usuario en su paso por la red (los cuales usualmente conllevan una buena cantidad de datos y metadatos que revelan su vida fuera de la red).
Estas herramientas, popularizadas a lo largo de los dos últimos años se presentan en diversas modalidades, siendo algunas ofrecidas a los usuarios como una forma de simplificar el manejo de las diversas manifestaciones de su personalidad virtual; mientras que otras son puestas únicamente al servicio de grandes corporaciones o Estados.

[385] Del inglés "Social Media Aggregator".

imposible) utilizar uno de estos dispositivos sin unificar en ellos nuestros diversos perfiles digitales[386].

Convertidos en una verdadera manifestación física de la convergencia de las telecomunicaciones, nuestros dispositivos electrónicos se presentan como un primer punto de inflexión, a partir del cual nuestra información personal es recopilada y agregada (por nosotros mismos o por los sistemas informáticos utilizados), para a continuación ser utilizada (con o sin nuestro conocimiento y/o consentimiento) como valor de intercambio en los mercados móviles[387].

Asimismo, esta tendencia cuenta también en la actualidad con diversas manifestaciones virtuales[388], las cuales comparten con sus contrapartes físicas la capacidad de recopilar un conjunto amplio de información proporcionada voluntariamente por parte de sus usuarios, a lo largo de sus diversas transacciones sociales en línea.

Independientemente del carácter material o inmaterial de la manifestación de los *agregadores de redes sociales* a los que se ha hecho referencia, la cruda realidad pone en evidencia que estos aumentan el riesgo de que los sujetos de datos sufran daños o

[386] Lo cual conlleva también implicaciones importantes desde el punto de vista de la seguridad de la información, pues el contar con un punto unificado de acceso a nuestra información personal multiplica el riesgo asociado con la pérdida o el robo de estos dispositivos.
[387] Los cuales sustentan la "venta" de aplicaciones gratuitas (sumamente populares en el mercado costarricense) en la cesión de los datos transaccionales, de localización y contextuales de sus usuarios a los desarrolladores o a terceras empresas que utilizan dicha información para (en el mejor de los casos) mostrar al usuario publicidad personalizada.
[388] Pudiendo encontrarse ya casos de redes sociales y sistemas operativos sociales virtuales que unifican la información social disponible en la red aún sin que el potencial usuario sepa de su existencia, para a continuación atraer su atención ofreciéndole conocer lo que la compañía "sabe" sobre él y "tomar el control" de su nuevo perfil unificado a cambio de una módica contraprestación monetaria (o incluso sin retribución alguna).

perjuicios a partir de las potenciales violaciones a la autodeterminación informativa que estos facilitan.

Así las cosas, la capacidad del marco regulatorio costarricense para reconocer y prevenir este nuevo conjunto de riesgos adquiere un carácter fundamental, y es especialmente importante a la hora de determinar el nivel de protección brindado por el sistema de protección de datos de nuestro país.

A pesar de ello, el panorama normativo costarricense no contempla disposiciones específicamente dirigidas a la protección de los intereses de los sujetos de datos frente a las redes sociales en tanto son consideradas servicios de información. Aun cuando cuenta efectivamente con algunos principios que procuran proteger al individuo ante el amplio panorama presentado por las redes sociales, el sistema costarricense de protección de datos personales puede ser caracterizado por omitir disposiciones relevantes (entre otros temas) al manejo de información personal en los mercados internacionales de aplicaciones, redes sociales y dispositivos informáticos[389], que posibilitan la agregación de información facilitada por el usuario de forma voluntaria.

Nuevamente, debereconocerse este carácter voluntario de la cesión como el problema fundamental que rodea al uso de estas herramientas sociales. A pesar de ello, un sistema de protección de datos realmente maduro, debería ser capaz de asegurar a sus usuarios la extensión completa de su derecho de acceso a la información (aun de

[389] En este punto debe señalarse como relevante el hecho de que nuestra Sala Constitucional considerara "las medidas tendientes a proteger la seguridad del usuario, frente a radiaciones no ionizantes y ante posibles ataques a la privacidad de las comunicaciones" (Sala Constitucional de la Corte Suprema de Justicia, 2011) como fundamento social al procedimiento de Homologación realizado por SUTEL a los dispositivos de telecomunicaciones móviles.

manera transnacional) y especialmente reconocer (y facilitar) los derechos de revocación y al olvido en toda su extensión.

Finalmente, debe resaltarse como significativo el que la Ley Nº 8968 establezca como atribución de la PRODHAB en el inciso j) de su artículo 16 únicamente el *"fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales"* (Asamblea Legislativa de la República de Costa Rica, 2011) y que a pesar de ello olvide afirmar la necesidad de que tanto esta institución, como otros entes relacionados, realicen campañas de información y concientización al usuario final sobre el manejo adecuado de la información que comparte en redes sociales.

### *Traición por Datos de Localización*

La problemática relacionada con los datos de localización es en la actualidad un problema vigente en nuestro país. Los datos de localización cuentan con un enorme potencial para identificar con exactitud a un usuario específico aún cuando se cuente con una cantidad limitada de información. Asimismo, tal como pudo evidenciarse a lo largo del análisis hecho a la normativa nacional e internacional, la normativa de telecomunicaciones vigente en Costa Rica obliga a todos los operadores y proveedores a recopilar, retener, e incluso a compartir los datos de localización de sus usuarios.

El manejo limitado de los datos de localización en los servicios de telecomunicaciones se encuentra regulado fundamentalmente en nuestro país por la Ley Nº 8642, la cual

establece en su artículo 43 que: *"Los datos de tráfico y de localización relacionados con los usuarios finales que sean tratados y almacenados bajo la responsabilidad de un operador o proveedor, deberán eliminarse o hacerse anónimos cuando no sean necesarios para efectos de la transmisión de una comunicación o para la prestación de un servicio. Los datos de tráfico necesarios para efectos de la facturación de abonados y los pagos de las interconexiones, podrán ser tratados hasta la expiración del plazo durante el cual pueda impugnarse, legalmente, la factura o exigirse el pago. Los datos de localización podrán tratarse solamente si se hacen anónimos o previo consentimiento de los abonados o usuarios, en la medida y por el tiempo necesario para la prestación de un servicio"* (Asamblea Legislativa de la República de Costa Rica, 2008).

A pesar de esta mención expresa a los datos de localización, a lo largo del presente estudio ha podido demostrarse que estos pueden ser vulnerados, tanto por los servicios de telecomunicaciones como por los servicios de información que se han visto unificados por medio de la convergencia de las telecomunicaciones. Por ello, el hecho de que la normativa específica del sector limite su ámbito de tutela únicamente a los servicios de telecomunicaciones, hace que el riesgo representado por estos para los usuarios finales se mantenga vigente[390].

De esta manera, puede concluirse este punto asegurando, con base en la experiencia[391] del suscrito autor de esta investigación, que a la fecha la tutela del

[390] Aún cuando se limitara este enfoque a los datos de localización tutelados por el artículo 43 supracitado, funcionarios de SUTEL (Méndez, Marín, & Steller, 2013) y de PRODHAB (Artavia Chavarría, 2014) han afirmado que a la fecha ha sido imposible garantizar el cumplimiento por parte de los operadores y proveedores de servicios de telecomunicaciones este deber de eliminación o anonimización.

[391] En tanto fue imposible identificar una investigación que versara sobre la aplicación real de las disposiciones normativas sobre protección de datos de localización en Costa Rica, parte de la presente investigación se dedicó a presentar los trámites necesarios para identificar la capacidad de un ciudadano ordinario de ejercer su derecho de acceso e información ante un operador de telecomunicaciones.

derecho de autodeterminación informativa no ha podido extenderse correctamente a la protección de los datos de localización transados por las comunicaciones convergentes en nuestro país. Ante tal situación, no queda otra opción que considerar que Costa Rica no cuenta por el momento con un nivel adecuado de protección de los datos de localización de sus ciudadanos.

### *Transferencias Internacionales de Datos Personales*

Considerado por muchos como el tema más delicado y de mayor relevancia para la protección de datos ante la convergencia de las telecomunicaciones, las transferencias internacionales de datos personales exponen la información personal a un conjunto amplio de riesgos que escapan a los ámbitos de protección brindada por los sistemas nacionales de protección de datos.

---

El día 14 de diciembre de 2012 fue presentada una solicitud ante el Instituto Costarricense de Electricidad relacionada con los datos de tráfico y localización que la compañía retenía sobre sus usuarios. La consulta buscaba determinar con qué facilidad podría un usuario final (encarnado en este caso por este investigador) obtener dicha información por parte de una sucursal regional.
Presentada de manera oral ante el coordinador de la agencia regional del instituto (con miras a emular el proceso comúnmente utilizado por un ciudadano ordinario) y fundamentada en las disposiciones de la Ley 8642 y la ley 8968, la consulta fue resuelta por medio de la nota 9160-AN-273-2012 (ver Anexo 10) de manera genérica y negativa.
Como respuesta a las solicitudes de información, la nota presenta al sujeto de datos con un conjunto de meras definiciones de lo que la ley determina como datos personales (sin adjuntar los datos específicos requeridos), a la vez que ignora la solicitud de liberar los datos de localización del usuario. Asimismo, requiere la nota el cobro de una tarifa con miras a la liberación de los datos de tráfico de llamadas alegando que *"en lo que respecta a la información requerida sobre las conexiones de datos y las radiobases a las que se conectó el servicio celular, debe indicarse al solicitante, que el ICE no guarda este tipo de registros" (Ver anexo 10).*
Ante esta situación, el 27 de diciembre de 2012 fue presentada una respuesta que recordaba la obligación impuesta por el artículo 7 de la ley 8642, de que el operador facilite un informe que detalle *"la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen"*. A la fecha no se ha recibido respuesta a dicha misiva.

Maximizadas por la cada vez mayor intrusión de las comunicaciones convergentes en nuestro país y el mundo, estas transferencias plantean un sinnúmero de problemas internacionales[392] que aún no han sido solucionados. A pesar de tan penosa realidad, el estudio referido con anterioridad del marco legal que rodea a la protección de datos en el plano internacional, evidenció la existencia de algunos instrumentos y sistemas que a la fecha han avanzado hacia la solución de estos problemas.

En este contexto, la capacidad de reacción y prevención del sistema costarricense de protección de datos dependerá, evidentemente, de su incorporación en las diversas iniciativas regulatorias y técnicas que procuran generar soluciones viables a esta problemática.

Un primer elemento por tomar en consideración a la hora de dilucidar el compromiso y la participación de nuestro país en estos elementos, puede encontrarse en la subscripción y ratificación de convenios y tratados internacionales vinculantes, dirigidos a generar marcos regulatorios estables (o interoperables) que superen la problemática ya planteada.

De conformidad con el análisis realizado al marco internacional de la protección de datos, el Convenio 108 del Consejo de Europa puede caracterizarse como el único tratado internacional abierto a su ratificación por cualquier país del orbe que contempla disposiciones vinculantes sobre la transmisión transfronteriza de datos personales. Así las cosas, el que Costa Rica no sea parte aún de este instrumento

[392] Mencionados a lo largo de la sección dedicada al tema en el segundo capítulo de la presente investigación.

internacional, se presenta como una grave omisión que debilita tanto la imagen de nuestro país como la capacidad de acción de PRODHAB en el ámbito internacional.

Tal como fue evidenciado a lo largo de la segunda sección del capítulo anterior, a la fecha Costa Rica no cuenta con sustento normativo suficiente como para generar una verdadera vinculación del sistema nacional de protección de datos personales, con el existente en el plano internacional[393]. De esta manera, la limitada gama de instrumentos normativos ratificados, aunada con los restringidos ámbitos de aplicación de estos plantea un panorama poco halagüeño para la implementación de soluciones reales a los problemas estudiados.

Partiendo de tal situación, la responsabilidad de proteger los intereses de los sujetos de datos en el plano internacional es depositada en su totalidad en el marco normativo interno, que rodea la protección de datos en las telecomunicaciones convergentes. En este contexto, adquieren suma importancia las disposiciones que sobre la materia contienen la Ley Nº 8968 y su reglamento, pues dependerá de ellas la adecuación de nuestro país a los altos estándares internacionales necesarios para garantizar una interoperabilidad efectiva[394].

Tal como recordará el lector, la transferencia de datos personales se encuentra regulada en nuestro país por una única regla general que establece la Ley Nº 8968 en su artículo 14, la cual afirma que: *"Los responsables de las bases de datos, públicas o*

[394] Debe mencionarse que en este punto adquiere gran relevancia nuestro estudio de los modelos nacionales ya estudiados que han basado sus sistemas en la adopción de normativa especializada pues nos permite observar al menos un ejemplo de la incorporación de los más altos estándares mundiales de protección de datos en un sistema normativo nacional sin que ello dependiera de la ratificación de convenios internacionales (Canadá).

*privadas, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley"* (Asamblea Legislativa de la República de Costa Rica, 2011).

Esta disposición fue posteriormente complementada por el respectivo reglamento[395], el cual dedica de sus artículos 40 al 43 al tema; define la transferencia a lo largo de su artículo 40 como: *"la comercialización de datos personales por parte, única y exclusivamente, del responsable que transfiere al responsable receptor de los datos personales" (Poder Ejecutivo de la República de Costa Rica, 2013)*. Asimismo, designa este artículo como condición fundamental para la transferencia el *"consentimiento expreso e informado del titular, salvo disposición legal en contrario, asimismo que los datos a transferir hayan sido recabados o recolectados de forma lícita y según los criterios que la Ley y el presente Reglamento disponen. Toda venta de datos del fichero o de la base de datos, parcial o total, deberá reunir los requerimientos establecidos en el párrafo anterior" (Poder Ejecutivo de la República de Costa Rica, 2013).*

Subsecuentemente, establece el Reglamento tres disposiciones básicas: la supeditación de las transferencias de datos personales al cumplimiento de los protocolos mínimos de actuación; la asignación sobre el responsable de la carga de la prueba sobre la conformidad de la transferencia a las disposiciones legales relevantes; y la necesidad de incluir en el contrato de transferencia al menos las mismas obligaciones para el responsable receptor, que aquellas que atan al responsable de la

[395] Una característica del Reglamento es que procura solventar los evidentes vacíos existentes en la Ley Nº 8968 en materia de transmisiones internacionales de datos personales estableciendo dentro de su ámbito de aplicación que *"Este Reglamento será de aplicación a los datos personales que figuren en las bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos, en tanto surtan efectos dentro del territorio nacional, o les resulte aplicable la legislación costarricense derivada de la celebración de un contrato o en los términos del derecho internacional" (Poder Ejecutivo de la República de Costa Rica, 2013)*.

transferencia. Finalmente, debe recordarse que el artículo 59 reconoce como causal del procedimiento de protección de datos el que: *"Se transfieran, a las bases de datos de terceros países, información de carácter personal de los costarricenses o los extranjeros radicados en el país, sin el consentimiento de sus titulares"* (Poder Ejecutivo de la República de Costa Rica, 2013).

El sistema de protección de datos personales costarricense concentra, en tan solo siete artículos, la totalidad de los preceptos normativos relevantes a la transferencia internacional de datos personales. En ellos, nuestro sistema brinda un nivel de protección que, en contraste con otros sistemas estudiados, resulta sumamente conservador[396].

Debe concluirse este apartado afirmando que, si bien es cierto que nuestro país es actualmente partícipe de varios de los foros y grupos mencionados a lo largo de la tercera sección del capítulo tercero de esta investigación[397], la realidad refleja un compromiso sumamente limitado por parte del Estado costarricense hacia la protección de los datos personales en el plano internacional.

Esta situación torna, por sí sola, imposible el considerar como adecuado el grado de protección brindado por nuestro país a los datos personales de los usuarios de

[396] Pues, a diferencia (por ejemplo) de la normativa europea (y especialmente de las propuestas de reforma estudiadas) no contempla mayores soluciones a los problemas que aquejan la aplicación extraterritorial de la legislación nacional; no asegura la extensión de su ámbito de aplicación a la protección de los nacionales con independencia del lugar de tratamiento; no reconoce disposiciones especiales para la transferencia extraterritorial de datos personales (con excepción de la necesaria reiteración de las cláusulas contractuales ya mencionada); y no prohíbe la transferencia de datos personales a países que no cuenten con un nivel adecuado de protección.

[397] Específicamente debemos reconocer la participación de nuestro país en grupos como la Red Iberoamericana de Protección de Datos y la buena disposición de miembros de MICITT, PRODHAB y SUTEL a participar en foros internacionales (tanto multilaterales como de múltiples interesados) de Gobernanza de Internet en los cuales han sido defendidos los derechos humanos y los principios básicos de la protección de datos personales.

tecnologías convergentes, pues al enfocar su mirada únicamente al interior, ignora el carácter transfronterizo y descentralizado de los flujos de datos que caracterizan las telecomunicaciones modernas.

### *Violaciones a la Autodeterminación Informativa por otros Estados*

Tal como podrá suponer el lector, el manejo de las violaciones a la autodeterminación informativa por otros Estados, se relaciona íntimamente con el punto anterior en tanto ambos se relacionan con el contexto internacional que rodea y limita la aplicabilidad de la protección de los datos personales.

De acuerdo con lo establecido a lo largo de la sección del capítulo segundo dedicada al tema, uno de los límites principales al derecho de autodeterminación informativa se encuentra en las excepciones legitimadas por motivos de seguridad nacional. Dirigidas originalmente a garantizar el bien común, estas excepciones han sido utilizadas recientemente para vulnerar masivamente los derechos individuales por parte de Estados en gigantescas operaciones de espionaje.

El papel de las TICs ha sido, por supuesto, fundamental para la realización de estas operaciones. Por ello, a nadie ha sorprendido la publicación, en los últimos años, de una cantidad cada vez mayor de noticias que confirman la existencia de poderosos sistemas de control, rastreo, recopilación y tratamiento de información personal en manos de las grandes potencias globales.

Gracias a las múltiples declaraciones de informantes como Edward Snowden y Julian Assange, actualmente el mundo es consciente del peligro que asecha a todo individuo por el mero hecho de utilizar herramientas tecnológicas en su diario vivir. En su afán por controlar y examinar los flujos transfronterizos de información, gobiernos como los de Estados Unidos, Rusia y China han desarrollado herramientas capaces de acceder a todo tipo de sistemas informáticos. Desde las grandes y seguras redes industriales de computación, pasando por elementos fundamentales de infraestructura, e incluyendo todos los sistemas de comunicación disponibles al público[398], actualmente pareciera que nadie se encuentra exento de la eterna vigilancia del *gran hermano*.

Esta amenaza no es ajena a los usuarios costarricenses, cuyos datos personales han sido ya puestos a la disposición del mejor postor (ver anexo 9) y que han sufrido el espionaje estatal en carne propia (ver *(Kozloff, 2013)*). Y es precisamente por ello que la posición adoptada por el gobierno costarricense ante estos fenómenos adquiere hoy, más que nunca antes, una gran importancia para la protección de datos personales.

Puede encontrarse un ejemplo importante de la necesidad de reacción estatal ante los eventos que amenazan la autodeterminación informativa de los usuarios, en la ya mencionada situación que rodeó las revelaciones publicadas en 2013 por Edward Snowden (las cuales pueden ser examinadas con más profundidad en *(Greenwald, MacAskill, & Poitras, 2013)*).

[398] Debe mencionarse en este punto que las revelaciones sobre el funcionamiento de los grandes sistemas de espionaje estatal publicadas por Snowden en 2013 no dieron lugar a dudas sobre la capacidad del gobierno estadounidense de acceder a toda la información contenida en todo tipo de dispositivos electrónicos en tiempo real gracias a la existencia de múltiples "puertas traseras" en el diseño de los dispositivos y de los estándares y protocolos utilizados por la esta industria.

Las violaciones a los principios del derecho internacional, aunadas con las violaciones a intimidad y a la autodeterminación informativa, justificaron fuertes reacciones por parte de los Estados[399]. En el plano global, estas reacciones incluyeron el generalizado de los Comisionados del Privacidad y Protección de Datos, quienes cumplieron con sus mandatos legales exigiendo activamente respuestas al gobierno estadounidense por sus actos. Lastimosamente, estas reacciones no fueron emuladas por el gobierno de Costa Rica (ni mucho menos por la entonces acéfala PRODHAB), el cual adoptó una posición *"extremadamente no conflictiva"(Kozloff, 2013)*, para a continuación procurar olvidar la situación tan pronto como fuera posible.

La pasividad del gobierno costarricense ante una situación que en otras latitudes ha sido considerada como intolerable, pone en evidencia de qué manera las limitaciones jurídicas del sistema nacional de protección de datos personales se relacionan también con elementos políticos. Condenado a sufrir embate tras embate de los múltiples problemas que aquejan a la protección de datos personales, el futuro de nuestro sistema dependerá, entonces, de un cambio en la voluntad política que posibilite la adopción de soluciones capaces de responder a los retos de la convergencia y al siempre cambiante contexto político internacional.

## Ubicación de Costa Rica frente a los Sistemas Internacionales Estudiados

[399] Siendo especialmente digno de mención el ejemplo Brasileño, cuya presidenta Dima Roussef manifestó expresa y activamente su descontento ante el espionaje sufrido por su pueblo e invitó a los miles de actores interesados a generar un documento que postulara los fundamentos de una buena gobernanza de Internet, el cual puede ser encontrado en: (Reunión Global de Multiples Interesados Sobre el Futuro de la Gobernanza de Internet "NETmundial", 2014)

Finalizado el examen de los puntos fundamentales que caracterizan el marco normativo nacional, se tiene ahora una perspectiva mucho más clara de la realidad de la protección de datos personales en Costa Rica. Gracias a ello, puede ahora culminarse el presente capítulo determinando, por medio de un breve análisis comparativo, el grado de tutela que brinda nuestro país al derecho de autodeterminación informativa en relación con el marco internacional ya estudiado.

Tal como fue establecido a lo largo del tercer capítulo de esta investigación, actualmente es posible identificar cuatro tendencias que marcan los diversos sistemas de protección de datos aplicados en el nivel mundial: la regulación mínima, la adopción de sistemas regulatorios regionales extensivos, la tutela por medio de habeas data, y la adopción de normativa especializada por parte de las diversas naciones. Cada uno de estos sistemas brinda diversos grados de protección a la información personal, por lo que podrán considerarse como un marco de referencia estable a partir del cual determinar si nuestro país cuenta efectivamente con una protección adecuada.

El sistema europeo de protección de datos, conocido por su amplio nivel de protección (basado en una intensa cooperación internacional) y por contar con un sistema de directivas de aplicación vinculante para los países miembros, plantea un primer punto de comparación. De conformidad con lo estudiado, los ciudadanos europeos se encuentran tutelados en la actualidad por más de once disposiciones normativas regionales (y un número considerable de disposiciones nacionales relevantes) que establecen todos los elementos necesarios para asegurar la tutela de su derecho de autodeterminación informativa dentro y fuera de las fronteras de la Unión.

Caracterizado por contemplar la protección de datos personales como un derecho fundamental y por contar con un alto nivel de refinamiento normativo y jurisprudencial, el sistema europeo representa en la actualidad el mayor referente internacional sobre la materia.

Con base en el estudio realizado sobre este sistema no queda duda que nuestro país cuenta aún con un largo camino por recorrer. Comparada con el marco normativo europeo, la normativa costarricense no se presenta como capaz de garantizar un nivel adecuado de protección a los datos personales (especialmente en el contexto de las telecomunicaciones convergentes). Ante esta realidad, solo es posible que los gobernantes y legisladores de nuestro país sigan el ejemplo europeo, reconociendo las debilidades de su sistema[400] y proponiendo un proceso serio dirigido a reformular y actualizarlo tan pronto como sea posible.

En segundo lugar, el ejemplo estadounidense cuenta aún con extrañas omisiones a los problemas demostrados a lo largo de esta y muchas otras investigaciones. Basado en el reconocimiento primordial de la libertad de expresión sobre el derecho a la privacidad (e incentivado en las últimas décadas por una incesante necesidad de controlar los flujos de información mundial), el sistema estadounidense cuenta actualmente con un buen número de normas positivas que (a pesar de su tendencia hacia la regulación mínima) regulan, con diversos grados de amplitud y especificidad, el uso de los datos personales por las diversas agencias federales.

[400] Debe recordarse que las propuestas de reforma planteadas actualmente en la Unión Europea que buscan actualizar la normativa general sobre protección de datos personales y establecer finalmente un marco normativo capaz de regular el tratamiento de datos personales por parte de entes judiciales y policiales.

A pesar de contar con estas disposiciones, el sistema federal estadounidense posee aún actualmente múltiples vacíos normativos que permiten las ya mencionadas "libertades" gubernamentales con respecto al manejo de datos personales, con los pretextos de la seguridad nacional.

Por otro lado, la regulación mínima se ve especialmente manifestada en la ausencia de normativa federal que limite realmente las potestades de tratamiento de datos personales por parte del sector privado, y si bien es cierto que algunas compañías han intentado superar esta situación apegándose al sistema de Safe Harbor, a la fecha es imposible encontrar en este país normativa general que tutele realmente los derechos de privacidad de los usuarios finales de telecomunicaciones convergentes, frente a todos los posibles vectores que amenazan su información personal.

De cara a este sistema, el marco normativo costarricense se posiciona en una evidente situación de ventaja (por lo menos desde el punto de vista de los sujetos de datos) pues aun cuando la Ley Nº 8968 cuenta con un ámbito de aplicación muy reducido, reconoce nacionalmente algunos de los principios y derechos relacionados con la autodeterminación informativa (la cual no es reconocida en EEUU sino como una posible extensión de la privacidad) y plantea límites claros al actuar de entes públicos y privados por igual.

En tercer lugar, el sistema basado en el reconocimiento del habeas data que ha sido implementado por algunos de los países latinoamericanos plantea un nivel básico de protección a los datos personales, al garantizar al sujeto de datos su capacidad de

ejercer los derechos subjetivos que configuran los elementos positivos del derecho de autodeterminación informativa.

A través de su evolución en los marcos normativos estudiados (Brasil, Paraguay, Perú, Argentina y Colombia), la protección brindada por esta garantía constitucional se caracterizó fundamentalmente por su carácter reactivo, y con el paso del tiempo, las tendencias internacionales aunadas con la constante evolución de las TICs evidenciaron la necesidad de complementar el habeas data con leyes específicamente dirigidas a garantizar la protección de los datos personales, bajo las modernas perspectivas dirigidas a prevenir, antes que reparar.

A pesar de que Costa Rica no llegó nunca a contar con el reconocimiento expreso por parte de nuestra Constitución Política acerca del habeas data, este fue garantizado a los interesados por medio de recursos de amparo que, tal como fue estudiado anteriormente, generaron una amplia gama de jurisprudencia constitucional relevante que aún hoy se encuentra vigente.

De esta manera, la relación que guarda nuestro país con las otras naciones que han adoptado el habeas data, es innegable. Si bien es cierto que en nuestro caso no se llegó nunca a profundizar tanto en el tema como en otras latitudes[401], la existencia de similitudes en el nivel de protección asegurado a los costarricenses por parte de nuestra Sala Constitucional, permite asegurar que durante esta etapa histórica nuestro país contó con un nivel de protección equiparable al existente en muchos de ellos[402].

[401] Debe recordarse aquí el ejemplo peruano donde fueron desarrollados diecinueve tipos de habeas data por medio de la jurisprudencia constitucional.
[402] Esta afirmación se basa única y exclusivamente en la consideración de los principios y derechos reconocidos a sus ciudadanos por parte de los países estudiados por medio del recurso de habeas data.

Tal como fue planteado con anterioridad, la última década se ha visto marcada por una creciente adopción de normativa especializada para la protección de datos por parte de las diversas naciones. Dirigida a complementar los sistemas ya existentes o a generar soluciones autóctonas ante la necesidad de garantizar los derechos individuales, esta tendencia ha generado múltiples ejemplos de sistemas normativos que presentan los más variados niveles de protección.

Con miras a reconocer esta situación y a generar un panorama claro en el cual poder ubicar los esfuerzos normativos que culminan en Costa Rica con nuestra propia ley especializada (Ley Nº 8968), el presente estudio condujo a examinar los sistemas legales de España, Canadá, México, Japón y China y a observar sus variaciones, según el contexto[403] que rodea a cada país.

Partiendo de los datos recopilados, el presente estudio permitió organizar estos países según el grado que poseen en materia de protección de datos. De esta manera, es posible ubicar a España como país líder en la lista, en tanto se ha visto obligado por las diversas directivas europeas a generar normativa especializada caracterizada por su gran calidad e interoperabilidad comprobada en el contexto de la Unión.

En segundo lugar, Canadá se presenta como un caso excepcional en el que la generación de legislación autóctona no ha limitado la capacidad de una nación de adoptar los más altos estándares internacionales. Con la certificación de protección

Evidentemente, con la posterior adopción por muchos de estos países de normativa dirigida a la regulación específica de la protección de datos personales esta situación de paridad se vio afectada.

[403] Y el grado de seriedad con el que ha sido abarcado el tema por parte de los respectivos gobiernos y legisladores.

adecuada otorgada por la Unión Europea, este país se ubica muy por encima de las iniciativas similares estudiadas.

A continuación, México recibe un tercer lugar en la clasificación en tanto reconoce constitucionalmente los derechos de acceso, corrección, cancelación y oposición y cuenta en la actualidad con un moderno marco legal que garantiza la protección de datos en el nivel federal.

Japón cuenta también con legislación específicamente dirigida a la protección de los datos personales, a pesar de lo cual el particular sistema de distribución administrativa que rige la aplicación de esta normativa y el hecho de requerir una actualización que le permita ajustarse al panorama tecnológico actual, ubican a este país en un cuarto lugar.

Finalmente, surge la obligación de a ubicar a China en el quinto y último lugar, en tanto no cuenta actualmente con un verdadero sistema de protección de datos personales. Tal como se estudió en el tercer capítulo, este país se encuentra aún en proceso de reconocer el derecho de sus ciudadanos a la intimidad y a la fecha cuenta únicamente con disposiciones indirectamente relacionadas con el tema.

Tal como podrá imaginar el lector, Costa Rica se asemeja en muchos aspectos a estos cinco países estudiados, en tanto su legislador ha optado por la creación de una ley específicamente diseñada para la regulación de la protección de datos personales. Tal como se ha señalado a lo largo de la presente sección, el sistema contemplado por la Ley Nº 8968 en nuestro país cuenta, a pesar de su reciente promulgación, con una redacción demasiado simple, que no ha sido capaz de regular correctamente

elementos tan fundamentales como las transferencias internacionales de datos personales y que limita excesivamente su ámbito de aplicación.

Tomando en cuenta este contexto y la totalidad de los elementos considerados a lo largo de esta sección, debe considerarse que el grado de protección brindado por el sistema costarricense lo ubica actualmente entre el tercero y el cuarto lugar de este *ranking.* Tal calificación podría verse justificada en tanto las características y límites contemplados por el ámbito de aplicación de la Ley Nº 8968 y su reglamento, no logran superar el nivel de protección brindado por el sistema mexicano, pero son un poco más extensos que los contemplados por el sistema japonés.

Asimismo, comparado con la complejidad y madurez lograda por los ejemplos de España y Canadá, el sistema de protección de datos costarricense pareciera encontrarse aún en pañales. Esta situación puede verse especialmente magnificada en el contexto generado por la convergencia de las telecomunicaciones, donde nuestro país no logra tutelar efectivamente los derechos de sus habitantes y encontrar soluciones a algunos de los problemas más básicos que se plantean.

Debe concluirse el presente estudio reconociendo que la respuesta a la pregunta: "¿Cuenta Costa Rica con un nivel adecuado de protección?", dependerá totalmente de la perspectiva desde la cual sea determinado el grado de protección necesaria para considerar adecuada la protección de datos personales. De esta manera, mientras que desde el punto de vista norteamericano la protección brindada por nuestro país podría parecer excesiva y capaz de vulnerar los principios del libre comercio; desde el punto de vista europeo la normativa nacional sobre la materia resulta insuficiente.

Considera el suscrito autor de este estudio, que tal situación puede ser solventada por la presente investigación adoptando el punto de vista de un usuario de tecnologías de telecomunicaciones convergentes. Desde esta perspectiva, los múltiples riesgos que plantean estas tecnologías para los ciudadanos costarricenses, aunados con la limitada gama de soluciones[404] previstas nuestro marco normativo, hacen que torne imposible considerar como adecuado el grado de protección brindado por el sistema costarricense de protección de datos.

[404] Se hace referencia en este punto, por supuesto, a las soluciones técnicas y jurídicas relevantes a las telecomunicaciones convergentes que puedan ser aplicadas de manera interoperable y transfronteriza para solventar estos problemas.

### *Síntesis de la Primera Sección*

*A lo largo de la cual es llevado a cabo un análisis crítico del marco normativo costarricense que rodea a la protección de datos personales en la convergencia de las telecomunicaciones.*

Manifestación de los Principios y Derechos Relativos a la Autodeterminación Informativa y la Protección de Datos Personales en el Marco Normativo Costarricense.

- Principios

  Los principios que enmarcan el derecho de autodeterminación informativa y la protección de datos personales no siempre corresponden con los vigentes en nuestro contexto, sino que han sido adoptados con diversos niveles de claridad por parte de la legislación costarricense de protección de datos personales, y han logrado manifestarse también dentro de las disposiciones positivas y jurisprudenciales que regulan las actividades del sector telecomunicaciones; a saber:

  - Principio de Libre Circulación de la Información: No contemplado directamente en la normativa nacional, manifestado en Ley Nº 7593 (art. 78) y Nº 4573 (arts. 196 y 196 bis).
  - Principio de Restricción Legítima: Plasmado en múltiples instancias del derecho nacional que incluyen nuestra Constitución Política (art.28) y la Ley Nº 6227 (art. 19).
  - Principio de Apertura: No contemplado expresamente por el marco regulatorio nacional, relacionado con la Ley Nº 8642 (art. 27).
  - Principio de Pertinencia: No previsto como tal por normativa relevante, citado por jurisprudencia constitucional (8996-02) y manifestado en Ley Nº 8968 (art. 6), Ley Nº 9162 y el reglamento de medidas de protección de la privacidad (art. 30).
  - Principio de Finalidad: Plasmado en la Ley Nº 8968 (art. 6) y recogido por jurisprudencia constitucional (04847-99), manifestado en Ley Nº 8642 (art. 43), Ley Nº 8968 (art. 6), Ley Nº 4573 (art. 196 bis), y reglamento a Ley Nº 8968 (artículo 4).

- Principio de Veracidad y Exactitud: Estudiado por la jurisprudencia constitucional (12239-04) y manifestado en Ley Nº 8968 (art. 6), Ley Nº 4573 (art. 236), reglamento a la ley Nº 8968 (arts. 12 y 23) y reglamento de protección al usuario final de telecomunicaciones (arts. 46, 57 y 58).
- Principio de Lealtad: Mencionado por jurisprudencia constitucional (8996-02) y contemplado por Ley Nº 8968 (art 4) y su reglamento.
- Principio de Transparencia: No ha sido planteado como tal por la legislación relevante, extrapolado de Ley Nº 8968 (arts. 5 y 7), reconocido por Ley Nº 6227 (arts. 2 y 3).
- Principio de Información: Reconocido expresamente como tal por Ley Nº 8968 (art. 5) y la jurisprudencia constitucional (8996-02), manifestado también en Ley Nº 8642, el reglamento a la Ley Nº 8968 (arts. 4, 12, 21, 38 y 39) y el reglamento de medidas de protección de la privacidad (arts. 7, 9, 10, 12, 13, 18, 25, 26, 30 y 32).
- Principio de Confidencialidad: Reconocido por la jurisprudencia constitucional (12239-04) y manifestado en Ley Nº 8660 (art. 35), Ley Nº 7566 (art. 12), Ley Nº 8968 (art. 11) y su reglamento (art. 31), reglamento de medidas de protección de la privacidad (arts. 1, 4 y 9), y el reglamento de protección al usuario final de telecomunicaciones (art. 6).
- Principio de Seguridad de los Datos: Recogido por la jurisprudencia constitucional (12239-04) y manifestado en Ley Nº 8642 (art. 42), Ley Nº 8968 (art. 10) y su reglamento (arts. 27-39), Ley Nº 9162 (art. 11), Ley Nº 7593, Reglamento de protección de la privacidad (arts. 3, 4, 6 y7).
- Principio de Prohibición de Procesamiento de Datos a Beneficio de Inventario: reconocido hasta cierto punto por la jurisprudencia constitucional (12239-04).
- Principio de Aseguramiento Técnico: Manifestado en Ley Nº 8968 (art 12) y su reglamento (arts. 33, 44 y 45).
- Principio de Licitud de los Criterios de Clasificación: Manifestado en Ley Nº 8968 (arts. 5 y 6).

- Principio de Defensa de los Datos Especialmente Protegidos: Retratado en Ley Nº 7593 (art. 78), Ley Nº 8968 (arts. 3, 9 y 31), Ley Nº 4573 (art. 196 bis) y Ley Nº 9162 (art. 11).
- Principio de Consentimiento: previsto como principio fundamental por la Ley Nº 8968 (art. 5) y manifestado en el reglamento a esta (cap. 2), la Ley Nº 8642 (arts. 43 y 44), Ley Nº 4573 (art. 196 bis), reglamento de protección al usuario final de telecomunicaciones (arts. 46, 57 y 58) y reglamento de protección de la privacidad (arts. 6, 9-13, 25, 26, 30 y 31).
- Principio de Responsabilidad: Identificable en la Ley Nº 8968 (arts. 3, 5, 6, 7, 10, 11 y 14) y su reglamento (art. 6).
- Principio de publicidad: Manifestado en las leyes Nº 8642 (art. 27), Ley Nº 8968 (arts. 16 y 21) y su reglamento (arts. 44-57).
- Principios de separación de poderes informativos y de control del procesamiento: No fueron encontradas referencias a estos principios en la normativa estudiada.

- Derechos Subjetivos:
  - Derecho de Acceso a la Información: Estipulado por nuestra Ley Nº 8968 (art. 7, Inciso 1) y su reglamento (art. 21).
  - Derecho de Rectificación: Encontrado en la Ley Nº 8968 (art. 7 inciso 2) y su reglamento (art. 23).
  - Derecho de Cancelación u Omisión: Dispuesto por Ley Nº 8968 (art. 7 inciso 2) y su reglamento (art. 25)
  - Derecho de Revocación: Establecido por la Ley Nº 8968 (art. 5, inciso 2), su reglamento (arts. 7-10) y el reglamento de protección de la privacidad (art. 25).
  - Derecho al Olvido: Reconocido por el reglamento a la Ley Nº 8968 (art. 19 y la ley Nº 8642.

<u>Técnicas y Herramientas de Protección de Datos en el Contexto Legal Costarricense</u>

- Técnicas de Seguridad de la Información: Se constituyen como parte fundamental de todo sistema de protección de datos personales en tanto aseguran técnicamente la información personal en las diversas etapas del tratamiento de los datos. Su incorporación en el plano normativo resulta necesaria pues asegura los mínimos por cumplir por parte de todas las bases de datos en el país.
    - Protocolos de seguridad de la información: Han sido regulados en el marco normativo costarricense fundamentalmente por medio del artículo 12 de la Ley Nº 8968 y los artículos 32, 33, 35 y 36 de su reglamento.
        - Registro de incidencias: Relacionado con Ley Nº 8968 (art. 32 inciso e) y normas técnicas para la gestión de las tecnologías de la información (punto 1.4.5).
        - Control de acceso, identificación y autenticación: Únicamente contemplado por Ley Nº 8131 y las normas técnicas para la gestión de las tecnologías de la información (punto 1.4.5).
        - Gestión de soportes y documentos: Herramienta aludida únicamente por las normas técnicas para la gestión de las tecnologías de la información (punto 1.4.4).
        - Herramientas de Control de Transferencias: Requeridas vagamente por la Ley Nº 8968 (art. 34) y mencionadas por las normas técnicas para la gestión de las tecnologías de la información (punto 1.4.4).
        - Procesos de Actualización: Contemplados fundamentalmente por el reglamento a la Ley Nº 8968 (art. 37).
    - Contratos y Cláusulas Modelo de Protección de Datos: Dirigidas a extender y facilitar la implementación de la protección de datos personales en el ámbito nacional, la creación y publicación de contratos y cláusulas modelo, es un servicio brindado usualmente por las autoridades reguladoras de protección de datos que responde a sus objetivos de educación y extensión. Se relacionan en nuestro país con la

Ley Nº 8968 (art. 16 incisos a), h) e i)), la Ley 8642 (arts. 41 y 46) y el Acuerdo de SUTEL sobre comunicaciones no solicitadas.

- Buenas Prácticas Corporativas: Resultado de acuerdos sectoriales dirigidos a ser implementados comúnmente. Han sido previstos por la ley Nº 8968 (art. 22).
- Autorregulación Vinculante: Promueve la adopción de compromisos normativos y técnicos, los cuales se tornan vinculantes mediante su registro ante el ente regulador, por lo que su incumplimiento puede ser penalizado según el régimen sancionatorio aplicable. Pese a su relevancia, no ha sido reconocida aún por nuestro país.
- Privacidad por Diseño: Herramienta de gran relevancia en la normativa internacional, requiere el respeto a la privacidad y la autodeterminación informativa en todas las etapas de los procesos implementados por entes públicos y privados. A pesar de ser compatibles con nuestro sistema jurídico, este omite totalmente cualquier referencia a estas herramientas.
- Ombudsman Corporativo/Institucional para la Protección de Datos Personales: Encargado de examinar continuamente los procesos realizados por su institución, el *ombudsman* labora en pro del cumplimiento de las disposiciones de protección de datos vigentes y la protección de los intereses de los titulares de los datos. Esta figura no ha sido contemplada por la normativa nacional relevante.
- Convenios Interinstitucionales: Herramienta que vincula al ente regulador con instituciones públicas y privadas con tal de facilitar sus labores. Se encuentra referenciado (vagamente) por la Ley Nº 8964 (art. 22).
- Referencias a Estándares Internacionales y Protocolos Técnicos: Herramienta necesaria para la correcta gestión de un sistema de protección de datos interoperable y actualizado. Nuestro país supedita a PRODHAB ante SUTEL en la determinación de las disposiciones técnicas aplicables al sector de las telecomunicaciones, por lo que se

vuelve fundamental la cooperación interinstitucional. Se encuentra determinado por la Ley Nº 8660 (arts. 2 y 6) y la Ley Nº 8960 (art. 16 incisos a), h) e i)) y cuenta actualmente con una única manifestación en la Resolución RCS-303-2012 (punto XVIII).

Grado de protección brindado en Costa Rica respecto al Derecho Comparado

*Donde son retomados los problemas relacionados con la convergencia de las telecomunicaciones y para analizarlos en el contexto normativo costarricense.*

- Proliferación de Cookies
    - Costa Rica ha experimentado un notable crecimiento en sus niveles de penetración de internet que lastimosamente no se ha visto acompañado de la educación necesaria para que la población comprenda el riesgo planteado por las cookies y otras técnicas similares de rastreo.
    - De conformidad con el experimento práctico realizado sobre el tema fue posible constatar que, al igual que sucede en otras latitudes, los usuarios costarricenses son rastreados sin su consentimiento en su paso por el mundo digital. Este rastreo se da a una escala impresionante, lo cual afecta sin duda alguna su derecho de autodeterminación informativa.
    - El marco normativo nacional no contempla disposición alguna que regule el uso de estas técnicas de rastreo y captura de datos transaccionales (dado que son normalmente utilizadas en el marco de los servicios de información), por lo que es necesario plantear las reformas necesarias para solucionar este problema. Una interpretación amplia de los principios planteados en la Ley Nº 8968 (art. 5) podría fundamentar tales limitaciones.
- Elaboración de Perfiles y Redes Sociales

- El notable surgimiento en el uso de internet móvil en Costa Rica ha aparejado un incremento importante en el número de usuarios de redes sociales, quienes cada día más las utilizan para ejercer sus derechos de información, libre expresión, comunicación y participación ciudadana.
- En este contexto los costarricenses son amenazados por las tecnologías y métodos dirigidos a canalizar toda la información generada por ellos hacia fines oscuros sin su consentimiento. Asimismo, la complejidad de manejar las múltiples manifestaciones de su personalidad virtual (cuentas, perfiles, avatares, y otros) han dirigido a los usuarios hacia la adopción de agregadores de redes sociales que toman actualmente formas aparentemente inocuas (ubicadas en los sistemas operativos de sus teléfonos celulares, por ejemplo).
- Frente a esta situación, aún cuando el panorama normativo costarricense contempla algunos de los principios y derechos relevantes, no logra proteger realmente los intereses individuales en los mercados internacionales de aplicaciones, redes sociales y dispositivos informáticos que posibilitan la agregación de la información voluntariamente facilitada por el usuario.
- Debe reconocerse este carácter voluntario de la cesión como el problema fundamental que rodea al uso de estas herramientas sociales. A pesar de ello, un sistema de protección de datos realmente maduro debería ser capaz de asegurar a sus usuarios la extensión completa de su derecho de acceso a la información (aun de manera transnacional) y especialmente reconocer (y facilitar) los derechos de revocación y al olvido en toda su extensión.

- Traición por Datos de Localización
  - La problemática relacionada con los datos de localización es, actualmente, un problema vigente en nuestro país. Los datos de localización cuentan con un enorme potencial para identificar con exactitud a un usuario específico aun cuando se cuente con una cantidad limitada de información.

  - El manejo limitado de los datos de localización se encuentra regulado fundamentalmente en nuestro país por la Ley Nº 8642 (art. 42). A pesar de la claridad de esta normativa, la presente investigación y las entrevistas con funcionarios de PRODHAB y SUTEL permitieron al suscrito investigador, determinar que a la fecha nuestro país no logra asegurar la correcta aplicación de estas disposiciones.
  - Esta situación es complicada por la inexistencia de regulación vinculante en el país para los servicios de información, pues estos conforman buena parte del riesgo para el usuario final.
- Transferencias Internacionales de Datos Personales
  - Las transferencias internacionales de datos personales exponen la información personal a un conjunto amplio de riesgos que escapan a los ámbitos de protección brindada por los sistemas nacionales de protección de datos; por ello, la incorporación del sistema nacional en las incentivas regulatorias y técnicas que procuran generar soluciones internacionales al tema se torna fundamental.
  - Frente a esta situación, el que nuestro país no sea miembro del convenio 108 del Consejo de Europa constituye un primer traspié para el tema. Esta situación es empeorada por la inexistencia de otros tratados internacionales que prevean disposiciones vinculantes realmente relevantes a los flujos transfronterizos de datos y por el carácter no vinculante de los acuerdos alcanzados por nuestro país en los diversos foros internacionales en que participa.
  - En el plano nacional, la situación no es mucho más esperanzadora, pues la única regla general que se refiere a las transferencias es establecida por la Ley Nº 8968 (art. 14), la cual es complementada por el reglamento a la ley (arts. 2, 40-43 y 59), por lo que la totalidad de nuestra normativa relevante se reduce a siete artículos que no logran realmente extender la protección de los datos de los habitantes de Costa Rica al ámbito internacional.
- Violaciones a la Autodeterminación Informativa por otros Estados

- Uno de los límites principales al derecho de autodeterminación informativa se encuentra en las excepciones legitimadas por motivos de seguridad nacional. Dirigidas originalmente a garantizar el bien común, estas excepciones han sido utilizadas recientemente para vulnerar masivamente los derechos individuales por parte de Estados en gigantescas operaciones de espionaje.
- Esta amenaza no es ajena a los usuarios costarricenses, cuyos datos personales han sido ya puestos a la disposición del mejor postor (ver anexo 7) y que han sufrido el espionaje estatal en carne propia (ver (Kozloff, 2013)). Y es precisamente por ello que la posición adoptada por el gobierno costarricense ante estos fenómenos adquiere hoy, más que nunca antes, una gran importancia para la protección de datos personales.
- Lamentablemente, hasta la fecha los gobiernos de nuestro país se han caracterizado por adoptar posiciones laxas y pasivas ante los escándalos recientes de espionaje, y en tanto no han llevado a cabo acciones realmente relevantes para defender los derechos de sus habitantes, resulta imposible afirmar como adecuada la protección brindada ante tales situaciones.

Ubicación de Costa Rica frente a los Sistemas Internacionales Estudiados

*Donde nuestro sistema de protección de datos es comparado con el grado de protección brindado por los siguientes sistemas:*

- Sistema Europeo: Sistema que asegura un alto nivel de protección a los datos personales (nacional, regional e internacionalmente), con respecto al cual la normativa nacional no se presenta como capaz de garantizar un nivel adecuado de protección (especialmente en el contexto de las telecomunicaciones convergentes).

- Sistema Estadounidense: Sistema caracterizado por procurar la mínima regulación de los temas relacionados con la protección de datos, con respecto al cual el marco normativo costarricense adquiere una evidente posición de ventaja (para los sujetos de datos) pues ha reconocido la importancia del tema y cuenta con normas dirigidas a regularlo en el nivel nacional.
- Sistemas basados en el Habeas Data: Implementado por algunos países de América Latina, este sistema brinda un grado de protección básico y de carácter tradicionalmente reactivo. Nuestro país comparte muchos de los elementos encontrados en este sistema y reconoció este recurso por medio de su jurisprudencia constitucional, por lo que en el pasado contó con un nivel equiparable de protección al de muchos de estos países.
- Sistemas que han adoptado normativa especializada: La adopción de normativa especializada ha respondido en el pasado reciente a la necesidad de muchos países de incorporar la protección de datos en sus marcos normativos (o de ampliar la protección brindada por otros medios).

  A lo largo de este estudio se han analizado cinco de los muchos países que han optado por esta solución, los cuales pueden ser organizados, según el grado de protección de sus respectivos sistemas, de la siguiente manera: 1) España, 2) Canadá, 3) México, 4) Japón, 5) China. Con base en lo estudiado a lo largo de la presente sección, puede considerarse que el grado de protección brindado por el sistema costarricense lo ubica actualmente entre el tercero y en el cuarto lugar de este ranking.

La respuesta a la pregunta "¿Cuenta nuestro país con un nivel adecuado?", depende de la perspectiva de quien determine este nivel. Desde el punto de vista del sujeto de datos potencialmente afectado por el mero uso de sistemas de telecomunicaciones convergentes, resulta imposible considerar que el grado de protección de datos personales brindado por el sistema costarricense, sea adecuado.

## Sección II: Recomendaciones

Una vez examinada la situación actual de nuestro país y detectados los vacíos existentes en su sistema de protección de datos personales, es conveniente plantear algunas recomendaciones que, de ser adoptadas, podrían contribuir a superar las limitaciones que impiden que nuestro país cuente con un grado de protección adecuado.

Relacionadas con los elementos normativos, técnicos, administrativos y políticos que determinan actualmente el rumbo de la protección de datos en Costa Rica, estas recomendaciones procurarán la aplicación de medidas necesarias en el corto, mediano y largo plazo, cuya urgencia ha quedado demostrada a lo largo de la presente investigación.

### *Medidas Necesarias a Corto Plazo*

1) Fortalecer la Agencia de Protección de Datos de los Habitantes.

En opinión de suscrito investigador, el fortalecimiento de PRODHAB es, en la actualidad, la primera medida que debe (y puede) ser adoptada por parte del gobierno de Costa Rica, con miras a asegurar la efectiva protección de los datos personales de sus habitantes.

A pesar de ser el principal ente regulador en materia de protección de datos del país y de contar con un conjunto relativamente extenso de obligaciones, desde su creación en 2011 PRODHAB se ha visto envuelta en una complicada serie de dificultades que ralentizaron el proceso de creación del reglamento a la Ley Nº 8968 y debilitaron a la Agencia en tanto impidieron su correcta entrada en funcionamiento.

Esta situación se extendió durante casi dos años durante los cuales la Agencia no contó con mayor presencia en el país y no fue sino hasta mediados de 2013 que PRODHAB pudo obtener algunos medios presupuestarios y humanos (con la designación de un par de funcionarios) que le permitieron comenzar a resolver el conjunto de problemas administrativos que hasta la fecha le acosan.

En la actualidad nuestro país cuenta con una institución que, aunque débil, lucha por cumplir con el importante papel que le ha sido asignado. Hoy la directora de PRODHAB trabaja porque le sean reconocidos mayores recursos[405] a la Agencia, a la vez que dedica su tiempo a reunirse con los diversos actores del sector con tal de impulsar la adopción de las prácticas requeridas por la Ley Nº 8968.

Por otra parte, debe reconocerse también que, pese a sus limitados recursos PRODHAB ha comenzado ya a cumplir con su responsabilidad de educar al público y de generar los convenios interinstitucionales necesarios para adoptar su posición dentro del panorama administrativo costarricense.

A pesar de la excelente disposición de sus funcionarios, no cabe duda del largo camino que aún debe ser recorrido por la Agencia, pues no solamente debe cumplir con las

[405] Y especialmente busca ampliar los recursos humanos de la institución.

obligaciones generales relacionadas con el registro y control de las bases de datos relevantes, sino que debe además, incentivar la protección de datos personales en aquellos mercados y tecnologías capaces de afectar la autodeterminación informativa de los habitantes de nuestro país.

Es en este punto donde la necesidad de fortalecer a PRODHAB se torna más relevante para el futuro de la protección de datos en la convergencia de las telecomunicaciones. Tal como lo se manifestó anteriormente, la normativa actual plantea algunas interrogantes sobre temas como la regulación técnica en materia de protección de datos en los servicios de telecomunicaciones, en la que el rol que debe cumplir PRODHAB aún no ha quedado totalmente claro (pues pareciera que debe cumplir un mero papel de asesoría para la toma de decisiones de SUTEL).

Este tipo de situaciones pone en entredicho el rol que debe cumplir PRODHAB en la actualidad, pues a pesar de haber sido creada con el fin único de proteger los datos personales de nuestros habitantes, la realidad demuestra que su ámbito de influencia es aun sumamente limitado.

Frente a esta dificultad, puede concluirse este punto afirmando que la necesidad de fortalecer PRODHAB se extiende tanto a garantizar que la institución cuente con los medios necesarios para cumplir con sus obligaciones, como a aclarar y ampliar su ámbito de control con tal de prevenir posibles conflictos con las diversas instituciones encargadas de regular sectores específicos. Asimismo, este fortalecimiento debe contemplar también la necesidad de que PRODHAB sea capaz de ejercer un control

más directo sobre las medidas técnicas de seguridad de la información por implementarse en las diferentes bases de datos bajo su tutela.

El fortalecimiento de PRODHAB deberá, por supuesto, acarrear mayores responsabilidades para la institución. La agencia debe procurar activamente la generación y el cumplimiento de los convenios interinstitucionales que le permitan participar activamente en la toma de decisiones que se relacionen con mercados específicos (no puede de esta manera escapar de su responsabilidad de acercarse a SUTEL con base en el hecho de que SUTEL no lo ha hecho primero).

Asimismo, este proceso debe también contemplar la ampliación del ámbito de aplicación de la Ley Nº 8968 con tal de asegurar la correcta inclusión de esta institución en todas las discusiones y negociaciones que puedan relacionarse con el manejo de datos personales. Un adecuado proceso de fortalecimiento institucional dirigido a solventar los problemas de generados por la convergencia de las telecomunicaciones en el país, debería generar una agencia de protección de datos de los habitantes capaz de hacer valer los derechos de los sujetos de datos ante cualquier ente, nacional o internacional, público o privado, que pueda afectarlos.

2) Ampliar la comunicación entre SUTEL y PRODHAB con tal de aclarar sus respectivos roles en la protección de datos en las telecomunicaciones convergentes.

Siguiendo el punto anterior, debe recordarse que la Ley Nº 8642 designa a SUTEL como ente responsable para el control del cumplimiento de las obligaciones de privacidad

impuestas a los operadores y proveedores de servicios de telecomunicaciones. Esta designación como ente regulador no contempla, sin embargo, la obligación de supervisar el cumplimiento de los proveedores de servicios de información[406] y esto genera dudas sobre la capacidad de SUTEL para tutelar de manera holística el respeto a los derechos de los usuarios de telecomunicaciones convergentes[407].

Frente a esta posibilidad, PRODHAB deberá asumir la responsabilidad de garantizar el derecho de autodeterminación informativa de los usuarios de los servicios de información que brinden o faciliten los operadores y proveedores de telecomunicaciones de nuestro país.

Con miras a cumplir esta responsabilidad, PRODHAB habrá de cooperar activamente con SUTEL en la identificación y supervisión de los servicios de información brindados por los actores del sector de telecomunicaciones en nuestro país. Asimismo, nuestra agencia de protección de datos deberá cooperar con SUTEL en el aseguramiento técnico de las tecnologías de telecomunicaciones convergentes que se pongan a disposición de los usuarios.

En otras palabras, dado su carácter de entidad reguladora especializada, PRODHAB no puede, bajo ninguna circunstancia, convertirse en un mero observador; sino que debe adoptar un papel activo y preventivo. Esta obligación se verá traducida, en el marco

[406] En este punto debe aclararse que nuestra Ley Nº 8642 establece en su artículo 51 la posibilidad de que SUTEL imponga ciertas medidas en los proveedores de servicios de información con tal de resguardar los derechos de los usuarios. A pesar de ello, las limitaciones establecidas por el artículo dejan en claro que no se está extendiendo a esta institución la obligación de garantizar la autodeterminación informativa o la protección de datos personales en los servicios de información.
[407] Especialmente en el contexto actual de las telecomunicaciones en nuestro país, en el cual es cada vez más común que los operadores y proveedores de servicios de telecomunicaciones brinden también servicios de información (como por ejemplo telefonía IP, mensajería multimedia, televisión por internet o por subscripción, y otros).

contextual de las telecomunicaciones convergentes, en la necesidad de que esta institución adopte como suya la tarea de regular las medidas de protección de datos aplicables en los servicios de información[408] y que acompañe a SUTEL en la tutela de los usuarios finales de los servicios de telecomunicaciones.

3) Reformar el Reglamento a la Ley Nº 8968.

En su forma actual, el Reglamento a la Ley Nº 8968 resulta problemático en tanto posee una serie de omisiones que dificultan las tareas de la Agencia de Protección de Datos. A lo largo de esta investigación se han podido identificar algunos de estos elementos conflictivos, dentro de los cuales se encuentran:

- Entender la nube como toda base de datos que es accedida por medio de Internet[409] y omitir disposiciones específicas sobre el tratamiento que pueda ser realizado en estas plataformas.
- Definir mediante el término "superusuario" una cuenta con perfil de ingreso y capacidad de lectura ilimitada[410] (lo cual ha generado grandes problemas prácticos para PRODHAB en la ejecución del requisito de inscripción (Artavia Chavarría, 2014)).
- Confundir el concepto de "base de datos interna, personal o doméstica" en su artículo tercero y no plantear claramente las circunstancias en las cuales dichas bases de datos se encontrarán exentas de registro.

[408] Medida que dependerá en gran medida de una futura reforma a la Ley Nº 8968 que logre superar los límites actualmente existentes en cuanto a su ámbito de aplicación.
[409] Sin mencionar el carácter descentralizado (y usualmente virtual) de estos sistemas.
[410] Tal como fue establecido anteriormente, un superusuario es aquel que posee la capacidad de realizar todo tipo de cambios al sistema sin restricción alguna.

- Reconocer un concepto sumamente limitado de la autodeterminación informativa que plantea fundamentalmente un conjunto de elementos reactivos, no preventivos.
- No regular correctamente las transferencias internacionales de datos personales, pues solo las menciona tangencialmente en su artículo (art. 59 inciso m.).
- No profundizar adecuadamente en las técnicas mínimas de seguridad de la información por utilizar, por parte de los entes regulados o en la capacidad de PRODHAB de exigir la implementación de mayores medidas al registrar los protocolos de actuación[411].
- No contar con disposiciones o recomendaciones relacionadas con los protocolos o estándares internacionales que deben dirigir las actuaciones de los entes regulados (ni brindar a PRODHAB la capacidad de determinarlos).
- No contemplar de manera completa los principios de la privacidad por diseño (específicamente a los principios de privacidad como configuración predeterminada, privacidad incrustada en el diseño, funcionalidad total, seguridad extremo a extremo, visibilidad y transparencia y enfoque en el usuario).

En tanto estas omisiones y disposiciones problemáticas dificultan las labores de la Agencia y limitan las acciones dirigidas a incentivar la protección de datos en el país, debe considerarse que en el corto plazo resultará fundamental la promoción de una

[411] Debe recordarse que en su artículo 35, el reglamento asigna la obligación de determinar las medidas de seguridad utilizadas a los encargados de las bases de dato, sin brindar mayores potestades a la agencia para exigir que mayores medidas (o de medidas específicas) sean implementadas en caso de ser necesario.

reforma[412] al reglamento que logre ampliar el grado de protección brindado, facilite el las labores de PRODHAB y asegure la mayor claridad y calidad posible en las disposiciones que rijan el manejo de los datos personales en nuestro país.

4) Promover la promulgación de reglamentos y directrices por parte de todos los entes relevantes para la protección de datos en tecnologías específicas.

De acuerdo con el estudio realizado del contexto administrativo de nuestro país, actualmente es posible encontrar un número significativo de instituciones y proyectos estatales que guardan relación con las telecomunicaciones convergentes y con el manejo de datos personales. De esta manera, ha podido observarse cómo actualmente nuestro país ha emprendido varios procesos que buscan incentivar la adopción de tecnologías como la nube, las firmas digitales y los expedientes digitales de salud en las actividades del sector público costarricense.

Ante esta realidad, el actual marco normativo nacional cuenta aún con una cantidad muy limitada de reglamentos y directrices que determinen los medios específicos que habrán de garantizar la protección de datos personales en estas nuevas tecnologías.

En opinión del suscrito autor de esta investigación, esta situación debe ser solventada mediante un esfuerzo consciente por parte de la administración pública, dirigido a asegurar la creación de normativa relevante por medio de un estudio claro y responsable de las nuevas tecnologías por implementarse. Asimismo, debe

[412] De acuerdo con los representantes de la Agencia, la necesidad de reformar el reglamento ya ha sido planteada, por lo que esta acción específica probablemente sea adoptada en el futuro cercano (Artavia Chavarría, 2014).

promoverse la inclusión de representantes de PRODHAB en la redacción de dichas disposiciones, a la vez que se favorece un marco de cooperación interinstitucional estable dirigido a asegurar el cumplimiento a largo plazo de las medidas generadas.

5) Desarrollar programas de inclusión de los diversos actores interesados en los procesos de protección de datos.

Tal como se mencionara con anterioridad, el proceso de creación del reglamento a la Ley Nº 8968 se vio afectado por una serie de dificultades que culminaron con la aprobación de un texto normativo que no generó mucha simpatía entre los sujetos regulados, pues ignoró muchas de las medidas recomendadas a lo largo de los procesos de consulta realizados[413].

A partir de las disposiciones de la Ley General de la Administración Pública y con base en la potestad de imperio de la administración de dictar normativa, no se puede asegurar que esta situación fuera de alguna manera irregular; sin embargo, no cabe duda de que su resultado final resultó poco conveniente, pues el texto final del

[413] Uno de los elementos que más resistencia causó durante el proceso de creación del reglamento a la ley Nº 8968 fue el hecho de que muchas de las observaciones de las partes e instituciones consultadas no se vieron traducidas en la versión final del documento.
Tal como se mencionara anteriormente, la Ley Nº 6227 establece, en su artículo 361 la posibilidad de que el poder ejecutivo conceda audiencias a las entidades descentralizadas, representativas de intereses de carácter general o corporativo e incluso al público en general en caso de que las disposiciones de carácter general que se encuentre elaborando pudiera afectar sus intereses.
De conformidad con este artículo, la consulta popular es actualmente una potestad discrecional de la administración pública. Esta particularidad, aunada con el hecho de que toda oposición o manifestación realizada por las partes consultadas no resultan actualmente vinculantes de manera alguna para la administración tiene como resultado la posibilidad de que, al igual que sucedió en el caso del reglamento a la ley Nº 8968, las disposiciones de carácter general finalmente aprobadas por el ejecutivo no satisfagan las necesidades de los administrados o generen conflictos a la hora de ser aplicadas.

reglamento contó aún con errores, señalados con la debida anticipación por las partes consultadas.

Tal como se ha analizado con anterioridad, la convergencia de las telecomunicaciones se ha visto aparejada en el mundo entero por una serie de cambios en los sistemas de gobernanza utilizados. Esta evolución ha significado la democratización de los procesos normativos, en tanto han garantizado una mayor inclusión de todos los actores interesados en los procesos que pueden afectarles.

Desde el punto de vista de la protección de datos personales, la inclusión y consideración de las posiciones de los actores interesados plantea interesantes opciones, en tanto garantiza medios activos de comunicación entre la administración pública y las instituciones y compañías reguladas, a la vez que permite el ejercicio de la democracia directa (planteada por nuestra Constitución Política en su artículo 9) mediante la incorporación del pueblo en la defensa de sus propios derechos.

Si bien es cierto que la potestad de imperio de la administración pública no puede ser negada (ni mucho menos reducida), es necesario asegurar mayores espacios dirigidos a la participación de los diversos actores interesados en los procesos de protección de datos personales, con miras a garantizar la puesta en común de los problemas y la búsqueda de soluciones novedosas mediante acuerdos de cooperación intersectorial[414].

6) Educar a la población mediante una fuerte campaña multimedia.

[414] Por medio de los cuales puedan ser generadas, por ejemplo, mejores prácticas corporativas vinculantes o programas de educación masiva copatrocinados por el sector público y privado.

De conformidad con las disposiciones de nuestra Ley Nº 8968, corresponde actualmente a PRODHAB la tarea de educar a la población en materia de protección de datos. Esta tarea debe ser realizada en nuestro país con la misma seriedad que la encontrada en otras latitudes, donde se han utilizado los medios más diversos para asegurar que las campañas masivas generadas no solamente llamen la atención de la población hacia los problemas, sino que generen también las capacidades necesarias para que los individuos mismos detecten y respondan ante potenciales amenazas a su información personal.

Lastimosamente, la educación de los ciudadanos en esta materia no es tarea fácil, pues los posibles vectores que amenazan la autodeterminación informativa en la convergencia de las telecomunicaciones son prácticamente infinitos. A pesar de esta dificultad, el ejemplo de otros países (especialmente los países europeos) ha demostrado que es posible inculcar en los ciudadanos algunas de las nociones generales por medio de su inclusión en todos los niveles de la educación (tarea que puede ser realizada por PRODHAB mediante convenios con el Ministerio de Educación y las diversas universidades del país).

Una vez que los ciudadanos cuenten con estas nociones básicas de protección de datos, nuestro país podrá contemplar posibilidades adicionales para educar a los usuarios de sectores o tecnologías específicas. Por medio de una futura expansión del marco normativo nacional sobre la materia, PRODHAB debería ser capaz de requerir[415] (al igual que lo hacen sus contrapartes europeas) que los proveedores de servicios de

[415] Nuevamente, este punto no debe verse simplemente como un elemento a ser adoptado dentro de las potestades de imperio de la administración, sino que puede ser generado también como parte de los acuerdos intersectoriales que sean facilitados por PRODHAB.

telecomunicaciones y de información generen o copatrocinen campañas de educación masiva y que incluyan en sus servicios todos los elementos necesarios para garantizar que sus usuarios comprendan realmente los riesgos y pasos por seguir para la protección de sus datos personales[416].

7) Fortalecer la inclusión de PRODHAB en la sociedad costarricense.

De la mano con las campañas de información planteadas en el punto anterior, la incorporación de PRODHAB dentro de la lista de instituciones en las que el costarricense promedio conoce y confía, resulta fundamental para la correcta aplicación de la protección de datos personales en nuestro país.

Con miras a asegurar dicha inclusión, la Agencia deberá generar en el futuro cercano programas de extensión capaces de mantener una fuerte presencia (en redes sociales, medios de comunicación y en las diversas comunidades) que garantice e incentive la participación y la retroalimentación ciudadana, a la vez que descentralice las actividades de enseñanza y comunicación de la agencia por medio de agentes multiplicadores (dirigidos a llevar los mensajes aún a las comunidades más alejadas).

El cumplimiento de estas tres recomendaciones abre un conjunto de interesantes posibilidades para la Agencia que no pueden ser menospreciadas. En primer lugar, la

[416] Este punto se relaciona intrínsecamente con el consentimiento del usuario y temas como las cláusulas leoninas que podemos encontrar en las diversas redes sociales y servicios de información provistos por entidades nacionales e internacionales.
Tal como lo plantean los principios de la privacidad por diseño, la educación del usuario es parte fundamental del consentimiento informado, por ello, todo servicio ofrecido en el contexto de las telecomunicaciones convergentes debe contar con las herramientas necesarias (videos explicativos, hipervínculos a cursos breves sobre el tema y "popups" en los que se manifiesten las tecnologías utilizadas) para asegurar que sus usuarios cuentan con toda la información necesaria que garantice dicho consentimiento y su habilidad de ejercer sus derechos.

presencia virtual de la Agencia de Protección de Datos de los Habitantes en las redes sociales abrirá canales bidireccionales de comunicación que permitirán a la Agencia atender de manera más eficiente las dudas de los sujetos de datos y a la vez llevar a cabo procesos de oficio de una manera más inteligente (al contar con un panorama claro sobre las tendencias generales que siguen los sujetos de datos).

En segundo lugar, su inclusión en los medios de comunicación servirá tanto para educar a la sociedad como para dar a conocer la Agencia. Mediante un correcto posicionamiento en los canales de comunicación masiva, PRODHAB podrá demostrar su interés de tutelar a capa y espada los intereses de los habitantes y esto a su vez le asegurará una mayor legitimidad ante los grupos sociales que pretende tutelar.

Finalmente, la Agencia podría seguir el ejemplo de la Privacidad por Diseño y la Oficina del Comisionado de Información y Privacidad de Ontario, creando su propio sistema de agentes multiplicadores[417]. Por medio de un proceso dirigido a educar y certificar gratuitamente a aquellos individuos, empresas y entes interesados en comprometerse a defender los principios de la protección de datos, PRODHAB podrá descentralizar sus funciones de comunicación y enseñanza y generar puntos de contacto entre los diversos sectores interesados en la protección de los datos personales.

8) Simplificar al máximo el proceso de denuncia.

[417] La adopción de este sistema constituye el máximo nivel de inclusión al cual puede actualmente aspirar nuestra Agencia actualmente, pues no solamente premia e incentiva la participación ciudadana en la promoción de la protección de datos sino que también crea una cadena de individuos y compañías comprometidos públicamente con la tutela de la autodeterminación informativa.

El último punto que debe ser implementado en el corto plazo se encuentra, tal como puede ver el lector, íntimamente relacionado con la totalidad de los elementos anteriormente estudiados. En el contexto actual de la protección de datos personales (y en los procesos de simplificación de trámites y de digitalización empleados por el Estado en medio de sus proyectos de *Gobierno Digital*) la simplificación de los procesos de denuncia debe ser prioridad fundamental para PRODHAB.

Con miras a lograr este objetivo, la Agencia deberá dar los pasos necesarios para garantizar que los sujetos de datos sean capaces de interponer sus denuncias por los más diversos medios, procurando lograr una simplificación similar a la encontrada en la jurisdicción constitucional en los recursos de habeas corpus (y de habeas data), e intentando incluso superarla por medio de la inclusión completa de la Agencia dentro de las redes sociales y las TICs.

### *Medidas Necesarias a Mediano Plazo*

1) Firmar y ratificar el Convenio 108 de la Unión Europea y e iniciar el proceso de renovación normativa que esto conllevaría.

El primer elemento que nuestro país debe considerar en el mediano plazo debe ser la firma y ratificación del Convenio 108 del Consejo de Europa. Tal como se ha establecido reiteradamente a lo largo de este trabajo; este tratado internacional se constituye actualmente en el único tratado internacional vinculante sobre protección de datos personales. Por ello su adopción implicará para nuestro país la necesidad

imperiosa de adecuar su normativa nacional a los estándares establecidos por el tratado (al igual que sucedió en materia de telecomunicaciones con la entrada en vigencia del CAFTA-DR en nuestro país).

Mediante la firma y la ratificación del Convenio 108, Costa Rica dará sus primeros pasos hacia la tutela real de los derechos de los usuarios de telecomunicaciones convergentes (en tanto estos dependen en gran medida de la capacidad del Estado de hacer efectivos estos derechos en el plano internacional). Asimismo, de ser implementada correctamente, esta acción podría constituirse en un elemento determinante que garantice en el futuro la obtención de la certificación de protección adecuada por parte de la Unión Europea.

Dado que la legislación nacional (salvo la Constitución Política) se encuentra supeditada a las disposiciones de los tratados internacionales, la incorporación completa y sin reservas de este tratado en nuestro marco normativo conllevará una serie de importantes cambios, entre los cuales se encuentran los siguientes:

- La extensión del ámbito de tutela del sistema de protección de datos personales en nuestro país a todas las categorías de datos en los ficheros y tratamientos automatizados de datos de carácter personal en los sectores público y privado[418].

[418] Sobrepasa de esta manera las limitaciones contempladas por el segundo párrafo del artículo segundo de la Ley Nº 8968, lo cual abriría múltiples posibilidades para PRODHAB. Entre ellas, quizá la más relevante para nuestros fines sería que la Agencia contará con la legitimación necesaria para tutelar correcta e ilimitadamente los derechos de los usuarios finales de servicios de información en el país.

- La incorporación de los principios básicos para la protección de datos establecidos por el capítulo segundo del Convenio en el derecho interno de nuestro país[419].
- La corrección de las limitaciones excesivas encontradas en la Ley Nº 8968.
- La incorporación en el marco normativo nacional de las disposiciones sobre flujos transfronterizos de datos encontradas en el capítulo III del Convenio[420].
- Recibir y brindar asistencia a los países miembros para el cumplimiento de la protección de datos[421].
- Brindar asistencia a las personas concernidas que tengan su residencia en el extranjero[422].
- Incluir disposiciones dirigidas a impedir posibles violaciones a la autodeterminación informativa por los países miembros[423].
- Eliminar las barreras monetarias actualmente existentes para el ejercicio de la protección de datos en el plano internacional[424].

[419] De acuerdo con el examen realizado a lo largo de la sección anterior, muchos de los principios plasmados por el Convenio ya han sido contemplados de una u otra manera en el marco normativo nacional. A pesar de ello, la firma y ratificación de este tratado tendrá como consecuencia la especificación clara del carácter de los mismos como principios generales de la protección de datos, lo cual resultará fundamental para la tutela efectiva de los derechos de los habitantes en el tratamiento casuístico en sede administrativa y penal.

[420] Las cuales incluyen los principios de libre circulación de la información, restricción legítima y apertura a la vez que incorporará la necesidad de requerir un grado de protección equivalente en el país receptor (y de impedir que por medio de sus fronteras sean generadas o replicadas transferencias que vulneren datos personales).

[421] Este elemento hará posible extender extraterritorialmente la protección brindada a nuestros habitantes de una manera fácil y clara, lo cual constituye un elemento fundamental para la protección de datos en las comunicaciones convergentes.

[422] Contraparte del punto anterior, garantiza la tutela extraterritorial de los datos de extranjeros en las bases de datos ubicadas en nuestro país.

[423] Con base en las disposiciones del artículo 15 del Convenio 108.

[424] Que pueden ser encontradas en tanto la mayor parte de los servicios de la información (y especialmente las redes sociales) cuentan dentro de sus términos de uso con cláusulas dirigidas a requerir que toda disputa o reclamación sea realizada en el país y la localidad donde la empresa se encuentra domiciliada.

Partiendo de todos estos elementos, la conveniencia del Convenio 108 para nuestro país resulta evidente[425], por lo que su firma y ratificación debe ser considerada un elemento prioritario de ser llevado a cabo en el mediano plazo.

2) Impulsar un proyecto de reforma a la Ley Nº 8968

Mientras que la reforma al reglamento de la Ley Nº 8968 planteará en el futuro cercano una nueva gama de posibilidades para la protección de datos en nuestro país, el estudio realizado de la normativa nacional permite identificar a la Ley Nº 8968 como principal causa de la problemática (por no decir dudosa) aplicabilidad de nuestro sistema en el contexto actual de las telecomunicaciones convergentes.

De acuerdo con lo estudiado anteriormente, nuestra actual Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales cuenta con una serie de limitaciones, dentro de las cuales se pueden encontrar las siguientes:

- Su ámbito de aplicación se encuentra demasiado limitado por las excepciones planteadas a lo largo del segundo párrafo de su artículo segundo y esta situación impide extender la tutela de la autodeterminación informativa a la

Por ello, en caso de que un usuario decidiera hacer efectivo su derecho de autodeterminación informativa no solamente enfrentaría los problemas relacionados con la tutela de sus derechos en un marco normativo que podría no reconocerlos como tales; sino también la gran carga monetaria que implicaría emprender un procedimiento legal (ordinario) ante tribunales extranjeros.

[425] Asimismo, en tanto las disposiciones del mismo no contemplan elementos extraordinarios, la adhesión de nuestro país al mismo no debería de causar recelo entre las instituciones y compañías reguladas.
Al contrario, debería de ser un incentivo importante para estas en tanto implicará la armonización de nuestro sistema de protección de datos con el encontrado en otros países y una simplificación importante en los trámites a seguir para la importación de datos personales desde Europa (y otros países), lo cual incentivará la capacidad de nuestro país para atraer inversión extranjera y brindar una mayor gama de servicios a los Estados miembros.

gran mayoría de los servicios de información a los cuales tienen acceso los usuarios en nuestro país.

- Cuenta con un conjunto sumamente limitado de definiciones (al punto de que su reglamento debió agregar un número importante de ellas).
- No comprende la totalidad de los principios relacionados con la autodeterminación informativa y la protección de datos[426].
- Contempla algunas excepciones a la autodeterminación informativa que podrían resultar excesivas.
- No menciona los metadatos dentro de su clasificación de los datos personales.
- Asigna la total responsabilidad sobre la determinación del contenido de los protocolos de actuación y las técnicas de seguridad por ser aplicadas a las empresas reguladas, sin reservar la posibilidad de que PRODHAB exija la incorporación de medidas más amplias o específicas.
- No cuenta con disposiciones específicamente dirigidas a regular los flujos transfronterizos de datos personales.
- Posee una limitada cantidad de disposiciones relevantes a las transferencias de datos personales.
- No cuenta con disposiciones relativas al ajuste de las medidas adoptadas por nuestro sistema con estándares internacionales (ni establece en ningún momento la necesidad de generar interoperabilidad con otros sistemas).
- No posee disposiciones relevantes a la privacidad por diseño u otros mecanismos similares.

[426] Incluyendo varias manifestaciones de estos principios, a pesar de lo cual no los recopila dentro de la sección dirigida a establecer los principios rectores.

- No requiere la inclusión de profesionales que fiscalicen y protejan los derechos de los usuarios dentro de las bases de datos corporativas e institucionales.
- No contempla la necesidad de regular específica y claramente las técnicas de protección de datos por ser implementadas en los servicios de información facilitados por las nuevas tecnologías.

A partir de todos estos elementos, el desarrollo e impulso de un proyecto de reforma a la Ley Nº 8968 debe constituirse en un elemento prioritario para nuestro país. Dicho proyecto deberá dirigirse a solventar los problemas encontrados en nuestra actual normativa y a la vez, a actualizar y ampliar el sistema de protección de datos costarricense.

Con miras a la promulgación de este proyecto de reforma, nuestro legislador deberá examinar las más recientes (y amplias) medidas de protección de datos generadas a lo largo del mundo, e incorporar sus disposiciones en un proyecto dirigido fundamentalmente a garantizar y certificar internacionalmente el grado de protección brindado por nuestro país a los datos personales.

Finalmente, puede afirmarse que, con miras a lograr la certificación europea de protección adecuada, nuestro país deberá asegurar que el cumplimiento de este punto sea logrado en unión con la firma y ratificación del Convenio 108 antes mencionado.

3) Fortalecer la cooperación regional con miras a la creación de marcos normativos comunes o interoperables en la materia.

Nuestro país es actualmente parte activa de varios foros regionales dirigidos a la protección de los datos personales (especialmente de la Red Iberoamericana de Protección de Datos) cuyas resoluciones y recomendaciones han marcado un importante precedente para la zona (aun cuando estas no sean vinculantes).

Por este motivo, nuestro país debe apuntar al fortalecimiento de los vínculos que le unen con estos foros internacionales, implementando efectivamente las recomendaciones con miras a garantizar su completo apoyo a la causa, e impulsando propuestas tendientes a unificar (o garantizar la interoperabilidad de) los sistemas de protección de datos de los países de la zona.

Finalmente, la participación de nuestro país en los diversos foros internacionales en los que actualmente participa, deberá encontrarse dirigida a la formación de bloques de países simpatizantes con la protección de datos personales. Asimismo, debe darse prioridad a la formación de tratados multilaterales o bilaterales que vinculen a la región y garanticen la tutela efectiva del derecho de autodeterminación informativa de sus habitantes.

4) Garantizar la capacidad de los sectores interesados en participar en los procesos nacionales e internacionales de toma de decisiones sobre el tema.

Relacionado (y dependiente de) la correcta puesta en práctica de las medidas de corto plazo 5, 6 y 7, este elemento requerirá que se garantice la capacidad de los diversos

sectores interesados (y especialmente de la sociedad civil)[427] de participar activamente (y de manera informada) en los procesos de toma de decisiones que afectan y dirigen las políticas, en temas relacionados con la protección de datos en la convergencia de las telecomunicaciones.

Nuestro país debe fomentar la información de nuestra sociedad sobre los eventos que afectan sus intereses, justificar públicamente las decisiones adoptadas por los delegados estatales que nos representan en estos foros, y facilitar la participación (sea presencial o remota) de todos los sujetos interesados en ellos. Esta obligación debe ser extendida desde el plano nacional[428] hasta el plano internacional[429].

[427] Es de reconocer en este punto que esta capacidad de participar activamente no se verá traducida necesariamente en la participación masiva de todos los sujetos afectados por la protección de datos personales, a pesar de ello resulta necesario que el Estado informe adecuadamente a la sociedad sobre los procesos que marcan las tendencias globales sobre el tema y garantice, en caso de ser necesario, que los individuos se manifiesten de manera legítima sobre aquellos temas que les afectan.
Puede considerarse esta situación retomando lo sucedido en el caso de las revelaciones de Edward Snowden en 2013. Tal como se afirmó anteriormente, en Estados Unidos y el resto del mundo, la información publicada por Snowden con respecto a los sistemas de espionaje masivamente implementados por este país contra el mundo entero acarreó graves consecuencias que se manifestaron rápidamente en el sentir popular.
Manifestado en la consternación masiva y las rápidas reacciones ciudadanas y diplomáticas que exigieron respuesta a la situación, el caso de Snowden tuvo graves consecuencias en la dirección macro política de la gobernanza de Internet, y sus efectos se hicieron sentir por igual en los foros de múltiples interesados como en los foros multilaterales del mundo.
Esta situación ha tenido consecuencias directas en la realidad de la protección de datos de los ciudadanos en tanto generó conciencia sobre las diversas vulnerabilidades que habían sido programadas hasta la fecha en los estándares abiertos (y específicamente en los sistemas de cifrado) que todos considerábamos seguros.
Es entonces donde puede observarse la relevancia de contar con un sistema que contemple no solamente la garantía de protección a los datos personales, sino también la capacidad de los sujetos tutelados de participar en los procesos nacionales e internacionales de toma de decisiones. El carácter democrático de nuestro sistema político requiere que, aun cuando nuestra participación individual sea ínfima, el Estado garantice nuestro derecho de participar y adoptar una posición sobre la conveniencia de las políticas que nos afectarán en el futuro.

[428] Por medio de la implementación de sistemas de participación remota en los procesos de consulta realizados por SUTEL, ARESEP, PRODHAB y demás instituciones relacionadas

[429] Por medio de la implementación de procesos de participación directa (informar al usuario sobre los medios disponibles para su participación en los foros globales) o indirecta (conduciendo consultas populares que revelen el sentir de los interesados respecto a temas específicos y manifestando dicho sentir en sus participaciones internacionales).

5) Incluir la privacidad por diseño tanto en el marco normativo nacional como en los métodos de actuación del sector privado.

Tal como se estudió anteriormente, la privacidad por diseño plantea la incorporación de un conjunto de elementos preventivos en todas las fases del diseño e implementación de los procesos generados por el sector público y privado. A partir de la reforma normativa ya planteada, y de los sistemas recomendados de cooperación intersectorial, todas las autoridades competentes deberán reconocer y educar a los actores interesados, en las ventajas que estas técnicas de protección de datos plantean para las empresas y sus usuarios.

Asimismo, deberán ser identificados aquellos actores nacionales e internacionales que más avance hayan logrado en la implementación de estas técnicas[430] con miras a reconocer su esfuerzo y formalizar acuerdos que permitan garantizar la correcta inclusión de la privacidad por diseño en nuestro país.

6) Crear e impulsar un proyecto de ley dirigido a regular los derechos de los usuarios de servicios de información en Costa Rica.

La actual desregulación de los servicios de información en el país plantea un conjunto complicado de retos para la protección de los derechos de los usuarios (y de los sujetos de datos en general) en tanto plantea elementos positivos y negativos a la vez. Por el lado positivo, contar con un marco normativo que no regule los servicios de información brinda una gran flexibilidad a los mercados digitales y facilita el

[430] Entre otros, deben formalizarse acuerdos con el Gobierno de Canadá y la oficina del Comisionado de Información y Privacidad de Ontario.

emprendedurismo. Por el lado negativo, esta situación puede verse (y usualmente se ve) aparejada de violaciones y abusos contra los usuarios de estos servicios.

Tomando en consideración el gran efecto que poseen estos servicios en la sociedad de la información (y con base en los estudios ya realizados sobre las telecomunicaciones convergentes, la protección de datos personales y el marco normativo nacional), nuestro país debe generar un proyecto de ley que regule el conjunto mínimo de derechos que deben ser asegurados a los usuarios de servicios de información en Costa Rica.

Dado el carácter multifacético de los servicios de información, es fundamental que este proyecto de ley se base en un proceso de formación, información y búsqueda de consenso que involucre directamente a los múltiples sectores interesados. Siguiendo el ejemplo del *Marco Civil da Internet*, nuestro proyecto deberá generar los medios necesarios para proteger los derechos fundamentales de los usuarios, sin que ello implique la imposición de cargas excesivas (o irracionales) a las empresas y los proveedores de servicios de información[431].

En otras palabras, este proyecto de ley deberá contemplar, entre otros temas posibles, disposiciones relativas a[432]:

- Los principios, derechos y obligaciones que regirán el uso de servicios de información en nuestro país (incluyendo entre otros temas el derecho al acceso

[431] Tal como se pudo observar a partir del ejemplo brasileño, la formación de un proyecto de esta magnitud no es simple. La generación de normativa por medio de procesos de múltiples interesados requiere de un alto grado de madurez política aunada con el apoyo de los tres poderes del Estado para su correcta implementación.
[432] Todos estos elementos pueden ser encontrados a lo largo del texto final del Marco Civil da Internet (Ley Nº 12965), cuya traducción no oficial puede ser examinada en (Rená, 2014).

al internet, a la información y el conocimiento, a la innovación y a las nuevas tecnologías).

- La nulidad de las cláusulas contractuales que violenten los derechos de los usuarios de servicios de información.
- Neutralidad de la red y neutralidad tecnológica.
- Intimidad, autodeterminación informativa y protección de datos personales.
- Retención de datos en servicios de información.
- Flujos transfronterizos de datos personales.
- Adopción de medidas de seguridad.
- Jurisdicción aplicable y resolución de conflictos.
- Propiedad intelectual.
- Educación.
- Multilingüismo.
- Rol de la administración pública.

Finalmente, debe admitirse que a pesar de la gran importancia de contar con legislación sobre este tema en nuestro país, el ejemplo brasileño nos muestra un método capaz de satisfacer a todas las partes involucradas por medio del consenso y la negociación. Tal como podrá imaginar el lector, este proceso no será ni fácil ni expedito; sin embargo, tiene el potencial de unificar, por fin, disposiciones que reconozcan y se adapten al carácter único del internet y los servicios de información con él relacionados.

### *Cambios Necesarios a Largo Plazo*

1) Procurar la obtención de una declaración de protección adecuada por parte de la Unión Europea para nuestro país.

Con base en la ruta de acción planteada anteriormente (y siendo realistas con el tiempo que durará nuestro país en implementar este conjunto de cambios), lograr que el grado de protección brindado por nuestro país sea certificado por la Unión Europea se nos plantea como una meta a largo plazo que, tal como se afirmó anteriormente, puede brindar grandes incentivos y beneficios a nuestro país.

Tal como podrá comprender el lector, la declaración de protección adecuada representará para Costa Rica su entrada a una etapa de madurez en la protección de datos personales. Ante tal perspectiva, para el momento en que sea obtenida esta certificación nuestro país deberá de contar con un sistema de protección de datos robusto, independiente y capaz de asumir luchas que superen las fronteras nacionales, con tal de tutelar los derechos de nuestros habitantes.

2) Posicionar a Costa Rica como un referente internacional de la protección de datos personales.

Mientras que la certificación europea de protección adecuada asegurará la capacidad de nuestro país de recibir y proteger correctamente la información personal, esta no debe ser vista como la solución a los problemas que enfrenta la protección de datos en la actualidad.

A lo largo de esta investigación se ha demostrado que el panorama de la protección de datos personales se encuentra perlado de clasificaciones, jurisdicciones, sistemas de protección de datos que dificultan y complican la puesta en práctica de las técnicas y herramientas de protección de datos. La convergencia tecnológica ha significado que los flujos transfronterizos de datos personales sean hoy parte inalienable de los sistemas de telecomunicaciones, con lo cual la delimitación de la protección de datos en dos planos (nacional e internacional) resulta incómoda e inoperante en la práctica.

Esta situación llama a la búsqueda de soluciones holísticas y globales al problema, y esas soluciones solamente podrán ser generadas mediante negociaciones y acuerdos internacionales que generen un grado mínimo de certeza, estandarización e interoperabilidad en los sistemas internacionales de protección de datos personales.

De conformidad con lo estudiado, los procesos de gobernanza que rigen actualmente las políticas mundiales de las telecomunicaciones y los servicios de información, se encuentran basados en los sistemas y foros multilaterales (ONU, ITU, OEA, IGF, y otros) y de múltiples interesados (ICANN, NetMundial, INET, IETF, y otros) que trabajan incansablemente por solucionar los problemas que acosan a la sociedad de la información.

Frente a tan intensa necesidad de cooperación internacional, en consideración del suscrito autor de esta investigación, nuestro país debe hacer lo posible por participar en tantos foros internacionales como sea posible, bogando siempre hacia la formulación de acuerdos que representen y respeten los mejores intereses de sus

ciudadanos[433] y haciendo honor a su tradición pacifista, asumiendo la mediación de aquellos conflictos que pudieran surgir, en la búsqueda de consensos.

Finalmente, es necesario concluir este punto afirmando la necesidad de posicionar a Costa Rica como un referente internacional de la protección de datos personales. Esta capacidad ya ha sido demostrada por nuestro país en el pasado, al participar y asumir roles de liderazgo en temas como la seguridad infantil en línea[434] y la promoción del multilateralismo[435]. Partiendo de tan ventajosa posición, las futuras administraciones deberán adoptar como propios los intereses de los usuarios de internet y de tecnologías convergentes, y liderar bajo esta bandera futuros movimientos internacionales de defensa y regularización de la protección de datos personales.

[433] Identificados por los procesos de consulta mencionados en la cuarta medida a ser implementada en el mediano plazo.
[434] Elemento asumido por la administración Chinchilla Miranda y gracias al cual nuestro país adquirió gran relevancia en las discusiones multilaterales sobre el tema ante entes como ITU y la ONU.
[435] Nuestro país es actualmente reconocido en los foros multilaterales (especialmente ICANN) gracias al énfasis brindado por la presidencia de la república al tema durante el discurso inaugural de la cuadragésima tercera reunión abierta de ICANN que se llevara a cabo en San José, Costa Rica en 2012.

## *Síntesis de la Segunda Sección*

Cambios Necesarios a Corto Plazo

1) Fortalecer la Agencia de Protección de Datos de los Habitantes.
    - Pese a ser el principal ente regulador en la materia, desde su creación PRODHAB se ha visto debilitada por un conjunto de problemas administrativos y presupuestarios que le han impedido, casi dos años después de su creación, comenzar a cumplir plenamente sus obligaciones.
    - Si bien la institución ha procurado realizar algunas actividades (como formalizar convenios interinstitucionales y comenzar sus tareas de educación), la agencia aún tiene un largo camino por recorrer, pues no solamente debe cumplir las tareas generales de protección de datos asignadas por la ley Nº 896, sino que debe también enfocarse en aquellos mercados y tecnologías que le resulten relevantes.
    - Actualmente la capacidad de PRODHAB de requerir la adopción de medidas técnicas por parte de los operadores y proveedores de servicios de telecomunicaciones es dudosa, dada la preponderancia de SUTEL en el área.
    - La necesidad de fortalecer PRODAHAB se extiende tanto a garantizar que la institución cuente con los medios necesarios para cumplir con sus obligaciones, como aclarar y ampliar su ámbito de control con tal de prevenir posibles conflictos con las diversas instituciones encargadas de regular sectores específicos.
2) Ampliar la comunicación entre SUTEL y PRODHAB con tal de aclarar sus respectivos roles en la protección de datos en las telecomunicaciones convergentes.
    - Siguiendo el punto anterior, debe recordarse que la Ley Nº 8642 designa a SUTEL como ente responsable para el control del cumplimiento de las obligaciones de privacidad impuestas a los

operadores y proveedores de servicios de telecomunicaciones. Esta designación como ente regulador no contempla, sin embargo, la obligación de supervisar el cumplimiento de los proveedores de servicios de información y esto genera dudas sobre la capacidad de SUTEL para tutelar de manera holística el respeto a los derechos de los usuarios de telecomunicaciones convergentes.

- Frente a esta posibilidad, PRODHAB deberá asumir la responsabilidad de garantizar el derecho de autodeterminación informativa de los usuarios de los servicios de información que brinden o faciliten los operadores y proveedores de telecomunicaciones de nuestro país.

3) Reformar el Reglamento a la Ley Nº 8968.

- En su forma actual, el Reglamento a la Ley Nº 8968 resulta problemático en tanto posee una serie de omisiones que dificultan las tareas de la Agencia de Protección de Datos, dentro de los cuales se encuentran:
    - Definir erróneamente la nube y omitir regularla.
    - Definir erróneamente el perfil de ingreso y lectura ilimitada como “superusuario”.
    - Confundir y no definir las circunstancias en que son válidas las excepciones por tratarse de bases de datos internas.
    - No regular las transferencias internacionales de datos personales.
    - No profundizar en las técnicas mínimas de seguridad de la información.
    - No establecer norma alguna en relación con los protocolos o estándares internacionales (o la posibilidad de que PRODHAB los determine).
    - No contemplar los principios de la privacidad por diseño.
- Por todos estos motivos debe recomendarse que sea reformado dicho reglamento, siguiendo un proceso que asegure la mayor claridad y calidad posible del producto final.

4) Promover la promulgación de reglamentos y directrices por parte de todos los entes relevantes para la protección de datos en tecnologías específicas.
    - A lo largo de esta investigación se pudieron identificar varios proyectos mediante los cuales nuestro país procura implementar nuevas tecnologías en las labores de la administración pública. Lastimosamente estos no han conllevado la generación de reglamentos o directrices que tutelen y especifiquen los procesos de protección de datos por ser utilizados. Por ello, debe fomentarse esta actividad por parte de la administración con el apoyo de PRODHAB.
5) Desarrollar programas de inclusión de los diversos actores interesados en los procesos de protección de datos.
    - Si bien es cierto que la potestad de imperio de la administración pública no puede ser negada (ni mucho menos reducida), es necesario asegurar mayores espacios dirigidos a la participación de los diversos actores interesados (y especialmente de la sociedad civil) en los procesos de protección de datos personales, con miras a garantizar la puesta en común de los problemas y la búsqueda de soluciones novedosas mediante acuerdos de cooperación intersectorial.
6) Educar a la población mediante una fuerte campaña multimedia.
    - De conformidad con las disposiciones de la Ley Nº 8968, corresponde actualmente a PRODHAB la tarea de educar a la población en materia de protección de datos.
    - Esta tarea debe ser realizada en nuestro país con la misma seriedad que la encontrada en otras latitudes, donde se han utilizado los medios más diversos para asegurar que las campañas masivas generadas no solamente llamen la atención de la población hacia los problemas, sino que generen también las capacidades necesarias para que los individuos mismos detecten y respondan ante potenciales amenazas a su información personal.
7) Fortalecer la inclusión de PRODHAB en la sociedad costarricense.

- De la mano con las campañas de información planteadas en el punto anterior, la incorporación de PRODHAB dentro de la lista de instituciones en las que el costarricense promedio conoce y confía, resulta fundamental para la correcta aplicación de la protección de datos personales en nuestro país.
- Con miras a asegurar dicha inclusión, la Agencia deberá generar en el futuro cercano programas de extensión capaces de mantener una fuerte presencia (en redes sociales, medios de comunicación y en las diversas comunidades) que garantice e incentive la participación y la retroalimentación ciudadana, a la vez que descentralice las actividades de enseñanza y comunicación de la Agencia por medio de agentes multiplicadores (dirigidos a llevar los mensajes aún a las comunidades más alejadas).

8) Simplificar al máximo el proceso de denuncia.
    - La Agencia deberá dar los pasos necesarios para garantizar que los sujetos de datos sean capaces de interponer sus denuncias por los más diversos medios, procurando lograr una simplificación similar a la encontrada en la jurisdicción constitucional en los recursos de habeas corpus (y de habeas data), e intentando incluso superarla por medio de la inclusión completa de la Agencia dentro de las redes sociales y las TICs.

<u>Cambios Necesarios a Mediano Plazo</u>

1) Firmar y ratificar el Convenio 108 de la Unión Europea y dar inicio al proceso de renovación del marco legal de la protección de los datos personales.
    - Tal como se ha establecido reiteradamente, este tratado internacional se constituye actualmente en el único tratado internacional vinculante sobre protección de datos personales. Por ello su adopción implicará para nuestro país la necesidad imperiosa de adecuar su normativa nacional a los estándares establecidos por el tratado.

- La incorporación completa y sin reservas de este tratado en nuestro marco normativo conllevará una serie de importantes cambios, entre los cuales pueden encontrarse los siguientes:
    - Incorporación de los principios básicos para la protección de datos encontrados en el Convenio en nuestro marco normativo.
    - Corrección a las limitaciones excesivas encontradas en la Ley Nº 8968.
    - Adopción de las disposiciones relativas a los flujos transfronterizos de datos personales.
    - Incorporación en el marco de asistencia para los países miembros y las personas concernidas creado por el Convenio.
    - Reconocimiento de disposiciones relativas a la prevención de violaciones a la autodeterminación informativa por los países miembros.
    - Eliminación de barreras monetarias.

2) Impulsar un proyecto de reforma a la Ley Nº 8968.

- Mientras que la reforma al reglamento de la Ley Nº 8968 planteará en el futuro cercano una nueva gama de posibilidades para la protección de datos en nuestro país, el estudio realizado de la normativa nacional permite identificar a la Ley Nº 8968 como principal causa de la problemática (por no decir dudosa) aplicabilidad de nuestro sistema en el contexto actual de las telecomunicaciones convergentes, en cuanto incluye limitaciones como:
    - Un ámbito de aplicación demasiado limitado.
    - Un conjunto limitado de definiciones.
    - No reconocer la totalidad de los principios relacionados con la autodeterminación informativa y la protección de datos.
    - Incluir excepciones excesivas a la autodeterminación informativa.
    - No mencionar los metadatos dentro de su clasificación de los datos personales.

- No asignar a PRODHAB capacidad de decisión sobre los protocolos de actuación y las técnicas de seguridad relevantes.
- No regular los flujos transfronterizos de datos personales.
- No regular satisfactoriamente las transferencias de datos personales.
- No vincular (o generar interoperabilidad) de nuestro sistema con los estándares internacionales apropiados.
- No reconocer los principios y herramientas de privacidad por diseño.
- No requerir la figura del *ombudsman de protección de datos*.
- No reconocer la necesaria regulación de las técnicas de protección de datos en los servicios de información.

- Debe propiciarse un proceso de reforma de la Ley Nº 8968 con miras a solucionar este conjunto de limitaciones y a lograr la certificación internacional de nuestro sistema de protección de datos personales.

3) Fortalecer la cooperación regional con miras a la creación de marcos normativos comunes o interoperables.
   - La participación de nuestro país en foros regionales dirigidos a la protección de datos personales debe ser fortalecida a la vez que son reforzadas nuestras relaciones con los países miembros, con miras a generar bloques de países simpatizantes con el tema.
   - Asimismo, nuestro país debe impulsar tratados multilaterales o bilaterales que unifiquen o garanticen la interoperabilidad de los sistemas de protección de datos de la zona.
4) Garantizar la capacidad de los sectores interesados en participar de los procesos nacionales e internacionales de toma de decisiones.
   - El país debe fomentar la información de nuestra sociedad sobre los eventos que afectan sus intereses, justificar públicamente las decisiones adoptadas por los delegados estatales que nos representan en estos foros, y facilitar la participación (sea presencial o remota) de todos los

sujetos interesados en ellos. Esta obligación debe ser extendida desde el plano nacional hasta el plano internacional.

5) Incluir la privacidad por diseño tanto en el marco normativo nacional, como en los métodos de actuación del sector privado.
    - A partir de la reforma normativa ya planteada y los sistemas recomendados de cooperación intersectorial, las técnicas y herramientas de privacidad por diseño deberán ser incorporadas en los sectores público y privado de nuestro país.
6) Crear e impulsar un proyecto de ley dirigido a la regular los derechos de los usuarios de servicios de información en Costa Rica.
    - La desregulación de los servicios de información plantea consecuencias positivas y negativas para nuestro país.
    - Tomando en consideración el gran efecto que poseen estos servicios en la sociedad de la información, nuestro país debe generar un proyecto de ley que regule el conjunto mínimo de derechos que deben ser asegurados a los usuarios de servicios de información en Costa Rica.
    - Este proyecto debe seguir el ejemplo del Marco Civil da Internet e incluir a los actores interesados en un proceso de redacción basado en consensos y participación popular.

<u>Cambios Necesarios a Largo Plazo</u>

1) Lograr declaración de protección adecuada por parte de la UE para nuestro país.
    - La declaración de protección adecuada representará para Costa Rica su entrada a una etapa de madurez en la protección de datos personales. Ante tal perspectiva, para el momento en que sea obtenida esta certificación nuestro país deberá de contar con un sistema de protección de datos robusto, independiente y capaz de asumir luchas que superen las fronteras nacionales con tal de tutelar los derechos de nuestros habitantes.

2) Posicionar a Costa Rica como un referente internacional de la protección de datos personales.
    - Frente al adverso panorama que afecta a la protección de datos personales en el plano internacional, Costa Rica debe participar activamente y liderar, de ser posible, la búsqueda de soluciones en los foros multilaterales y de múltiples interesados relevantes.
    - Nuestro país ya ha liderado movimientos internacionales en temas como la promoción del multilateralismo y la seguridad infantil en línea. Partiendo de tan ventajosa posición, las futuras administraciones deberán adoptar como propios los intereses de los usuarios de internet y de tecnologías convergentes, y liderar bajo esta bandera, futuros movimientos internacionales de defensa y regularización de la protección de datos personales

# Conclusiones Generales

Gracias al cumplimiento de los objetivos generales y específicos planteados al inicio de esta investigación, se ha podido comprobar la validez de las hipótesis planteadas y generar un conjunto de conclusiones que procuran sintetizar el estado actual de la protección de datos en la convergencia de las telecomunicaciones en Costa Rica y el mundo; a saber:

1) El reconocimiento de la dignidad y personalidad individual como fundamento de los derechos humanos surge a partir de una larga evolución histórica que aún sigue produciéndose. El actual reconocimiento internacional de los derechos humanos aunado con el exponencial crecimiento de las tecnologías de la información y la comunicación, han logrado poner en evidencia la necesidad de expandir la protección de los derechos otorgados a la persona humana más allá del mundo físico y adentrarse en la protección de la personalidad virtual.

   En este contexto, es también posible afirmar que actualmente existe un consenso cada vez más generalizado en el ámbito internacional, sobre la necesidad de reconocer la autodeterminación informativa como un derecho humano, distinto de los derechos de Intimidad, Privacidad e Información.

2) Actualmente la protección de datos personales comprende un conjunto de técnicas y herramientas. Estas procuran tutelar el derecho de

autodeterminación informativa mediante la adopción de una perspectiva iusinformática que se caracteriza por ser interdisciplinaria, holística y fundamentalmente preventiva.

Actualmente la protección de datos personales no se encuentra limitada únicamente a la protección de determinados tipos de datos, sino que se extiende a todos aquellos que rodean al individuo y que pueden ser contextualizados e interrelacionados para identificarle. Asimismo, esta protección debe ser extendida a todas las etapas del proceso de tratamiento de los datos personales.

3) A lo largo de su historia, los seres humanos han desarrollado sistemas de comunicación cada vez más complejos y sofisticados. A partir del surgimiento de las telecomunicaciones modernas estos sistemas han evolucionado de manera vertiginosa, superando su inicial carácter centralizado y vulnerable para tornarse en las novedosas *redes de nueva generación*, definidas por su carácter descentralizado, eficiente y fundamentalmente transfronterizo.

   Esta evolución ha dado lugar a la llamada *convergencia de las telecomunicaciones*, la cual no solamente representa la capacidad técnica de brindar múltiples servicios de información y telecomunicación por un mismo medio, sino que se ha visto aparejada con un complejo conjunto de cambios regulatorios, económicos, políticos y sociales que redefinen el funcionamiento del sector de las telecomunicaciones y su relación con los usuarios finales.

4) La convergencia de las telecomunicaciones tiene como consecuencia el surgimiento de una serie de riesgos para los intereses de los usuarios finales de servicios de información y telecomunicaciones. Esta situación afecta directamente a los habitantes de Costa Rica, quienes se mantienen en constante vulnerabilidad, dada la limitada protección brindada por nuestro actual sistema de protección de datos.

   El carácter transfronterizo de los datos transados, aunado con el tratamiento, transmisión y retención de cantidades cada vez mayores de información por Estados y entes privados por igual, ha sido objeto de fuertes discusiones en los más diversos foros internacionales. Esta situación ha generado también múltiples iniciativas de cooperación que, a pesar de los avances realizados, no han logrado plantear soluciones definitivas.

5) A lo largo de la presente investigación se han identificado cuatro tendencias seguidas en el derecho comparado que reconocen y tutelan de variadas maneras la protección de datos y la autodeterminación informativa. Lastimosamente, la existencia de tal diversidad normativa plantea serias dificultades para la tutela de los datos y metadatos personales que forman parte de los flujos transfronterizos característicos de las telecomunicaciones convergentes.

Frente a esta realidad, actualmente es posible identificar potenciales soluciones en las propuestas de coordinación, interoperabilidad y cooperación internacional, el planteamiento de tratados internacionales sobre protección de datos personales y la implementación de las más diversas soluciones técnicas.

6) Nuestra Ley General de Telecomunicaciones y su normativa conexa brindan un nivel aceptable de protección a los datos personales de los usuarios finales de los servicios de telecomunicaciones en el ámbito nacional. Sin embargo, en tanto el marco normativo costarricense del sector telecomunicaciones no regula los servicios de información, resulta imposible asegurar la correcta tutela de los datos personales tranzados en la prestación de estos servicios (especialmente en aquellos basados en flujos transfronterizos de información).

7) A pesar de su reciente promulgación, tanto la Ley de Protección de la Persona frente al tratamiento de sus datos personales como su reglamento, cuentan con un número importante de limitaciones, omisiones y vaguedades que impiden su correcta aplicación en las bases de datos no comerciales, los servicios de información y los flujos transfronterizos de datos personales, entre otros. Esta tendencia se puede ver replicada a lo largo de la normativa conexa relevante.

Dada la difícil situación que enfrenta la Agencia de Protección de Datos de los Habitantes y la limitada gama de convenios internacionales vinculantes con que cuenta nuestro país sobre el tema, resulta imposible afirmar que Costa Rica asegure una protección adecuada de los datos personales en las telecomunicaciones convergentes.

8) Las medidas recomendadas para el corto, mediano y largo plazo se encuentran dirigidas a dar solución a los problemas señalados y a impulsar el nivel de protección brindado por nuestro país a los datos personales, con tal de alcanzar los más altos estándares mundiales.

   Dentro de las soluciones recomendadas, debe recalcarse la importancia de reformar la Ley Nº 8968 y su reglamento; la firma y ratificación del Convenio 108 del Consejo de Europa; y la generación de un proyecto de ley dirigido a declarar los derechos de los usuarios de servicios de información en el país siguiendo el ejemplo del Marco Civil da Internet brasileño.

# Bibliografía

Katz v. US., 386 US 945 (Corte Suprema de Justicia de los Estados Unidos de América 1967).

Aboso, G. E. (Abril de 2005). Cibercriminalidad y derecho penal: el nuevo paradigma de la sociedad moderna. *Ley, razón y justicia. Revista de Investigación en Ciencias Jurídicas y Sociales*(9), 241-277.

Abramson, L., & Godoy, M. (14 de Febrero de 2006). *The Patriot Act: Key controversies.* Recuperado el 30 de Agosto de 2013, de Página web de NPR: http://www.npr.org/news/specials/patriotact/patriotactprovisions.html

Ackerman, S. (21 de Agosto de 2013). *NSA illegally collected thousands of emails before FISA court halted program.* Recuperado el 29 de Agosto de 2013, de The Guardian: http://www.theguardian.com/world/2013/aug/21/nsa-illegally-collected-thousands-emails-court

Agencia Central de Inteligencia. (07 de Enero de 2014). *The world factbook - Costa Rica.* Recuperado el 25 de Enero de 2014, de Página web de la Agencia Central de Inteligencia: https://www.cia.gov/library/publications/the-world-factbook/geos/cs.html

Agencia Española de Protección de Datos. (19 de enero de 2008). *Real decreto por el que se aprueba el reglamento de desarrollo de la ley orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal.* Recuperado el 03 de Octubre de 2013, de Página web de la Agencia Española de Protección de Datos: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf

Agencia Española de Protección de Datos. (19 de Enero de 2008). *Reglamento de desarrollo de la ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.* Recuperado el 03 de Octubre de 2013, de Boletín oficial del estado: http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

Agencia Española de Protección de Datos. (08 de Enero de 2010). *Real Decreto 3/2010.* Recuperado el 03 de Octubre de 2013, de Página web de la Agencia Española de Protección de Datos: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/art.81.5b_RDLOPD.pdf

Aguilar Bulgarelli, O. (1996). *Secreto de estado y el Derecho a la Información.* San José: Progreso Editorial.

Aguilar Cuevas, M. (1998). *Las tres generaciones de los Derechos Humanos.* Recuperado el 04 de enero de 2013, de Instituto de Investigaciones Jurdicas - UNAM: http://www.juridicas.unam.mx/publica/librev/rev/derhum/cont/30/pr/pr20.pdf

Aguilar Porras, A., & Tenorio Calvo, P. (2010). *Concesiones en telecomunicaciones - Telefonía móvil, a la luz de las leyes 8642 y 8660, y sus respectivos reglamentos. Trabajo final de graduación para optar por el grado de Licenciatura en Derecho.* San José : Universidad de Costa Rica.

Alcántara, J. F. (2008). *La sociedad de control - Privacidad, propiedad intelectual y el futuro de la libertad.* Barcelona: El Cobre.

Aldana J., A. T., & Vallejo C., A. (2010). *Telecomunicaciones, Convergencia y Regulación.* Recuperado el 25 de Octubre de 2013, de Revista de Economía Institucional: http://www.economiainstitucional.com/pdf/No23/aaldana23.pdf

Alessandri R., A., & Somarriva U., M. (2011). *Derechos de la Personalidad .* Recuperado el 16 de Febrero de 2013, de vlex.com: http://doctrina.vlex.cl/vid/derechos-personalidad-275058131

Allagui, I., & Kuebler, J. (2011). *The arab spring and the role of ICTs.* Recuperado el 06 de Abril de 2014, de Google Scholar - International Journal of Communication: http://scholar.google.com/scholar_url?hl=es&q=http://ijoc.org/index.php/ijoc/article/download/1392/616&sa=X&scisig=AAGBfm3bQS82ILdDNMAwK-1MJy7bEHmLJg&oi=scholarr

Alonso Salterain, S. (Septiembre de 2008). Las comunicaciones móviles. *Revista del Derecho de las Telecomunicaciones e Infraestructuras en Red*(33), 67-77.

Álvarez Ledezma, M. (1998). *Acerca del concepto derechos humanos.* México: Mc Graw-Hill.

American Civil Liberties Union. (Agosto de 2004). *The surveillance-industrial Complex: How the American Government is conscripting businesses and individuals in the construction of a surveillance society.* Recuperado el 20 de Marzo de 2012, de www.aclu.org: www.aclu.org/FilesPDF/surveillance_report.pdf

Anderson, N. (20 de Enero de 2012). *Explainer: how can the US seize a "Hong Kong site" like Megaupload?* Recuperado el 21 de Enero de 2014, de Ars Technica: http://arstechnica.com/tech-policy/2012/01/explainer-how-can-the-us-seize-a-hong-kong-site-like-megaupload/

Anthony Bowen, J. (Agosto de 2011). Cloud Computing: Issues in Data Privacy / Security and Commercial Considerations. *The Computer & Internet Lawyer, 28*(8), 1-8.

Antillón Montealegre, W. (07 de enero de 2013). Entrevista consultiva sobre Positivismo Jurídico e Historicismo Jurídico. (A. Quesada Rodríguez, Entrevistador)

Arias Cordero, A., & Chaves Rodríguez, H. (2010). *Los derechos fundamentales contenidos en el marco jurídico que regula las telecomunicaciones del país después de la promulgación del Tratado de Libre Comercio con Estados Unidos y sus leyes complementarias. Trabajo final de graduación.* San José: Universidad de Costa Rica.

Arias, J. P. (20 de Marzo de 2013). *Costa Rica tiene 4.6 millones de habitantes, según corrección del Censo 2011.* Recuperado el 20 de Enero de 2014, de www.elfinancierocr.com: http://www.elfinancierocr.com/economia-y-politica/Censo_2011-INEC-Centro_Centroamericano_de_Poblacion-correccion_0_266373372.html

Artavia Chavarría, N. (07 de Mayo de 2014). Entrevista sobre PRODHAB. (A. Quesada Rodríguez, Entrevistador)

Asamblea Legislativa de la República de Costa Rica. (01 de Enero de 1888). *Ley Nº 63 "Código Civil".* Recuperado el 28 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=15437&nValor3=90115&param2=2&strTipM=TC&lResultado=13&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (22 de Octubre de 1943). *Ley Nº 17 "Ley Constitutiva de la Caja Costarricense del Seguro Social".* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=2340&nValor3=84123&param2=1&strTipM=TC&lResultado=1&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (19 de Septiembre de 1963). *Ley Nº 3146 Tratado multilateral de libre comercio e integración económica latinoamericana.* Recuperado el 22 de Enero de 2014, de SUTEL - Normativa Internacional: http://www.sutel.go.cr/Medios/Descargar/1A61BCEDBCCE19BD3ABE96ED3609DDEC9E879945

Asamblea Legislativa de la República de Costa Rica. (29 de Abril de 1964). *Ley Nº 3284 "Código de Comercio".* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=6239&nValor3=89980&param2=1&strTipM=TC&lResultado=4&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (23 de Diciembre de 1967). *Ley Nº 4031 Tratado Centroamericano de Telecomunicaciones.* Recuperado el 22 de Enero de 2014, de Superintendencia de Telecomunicaciones - Normativa internacional: http://www.sutel.go.cr/Medios/Descargar/BF9AC34CF8090924DE4EC58D7DD12168D2E20141

Asamblea Legislativa de la República de Costa Rica. (15 de Noviembre de 1970). *Ley Nº 4573 "Código Penal".* Recuperado el 28 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=96389&param2=1&strTipM=TC&lResultado=10&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (03 de Mayo de 1971). *Ley Nº 4755 "Código de Normas y Procedimientos Tributarios".* Recuperado el 01 de Mayo de 2014, de Página web del Ministerio de Hacienda: http://www.hacienda.go.cr/centro/datos/Ley/Codigo%20de%20Normas%20y%20Procedimientos%20Tributarios-Ley%204755.pdf

Asamblea Legislativa de la República de Costa Rica. (28 de Septiembre de 1971). *Ley Nº 4806 Autoriza adhesión acuerdo sistema comercial de telecomunicaciones via satélite.* Recuperado el 22 de Enero de 2014, de Sutel - Normativa Internacional: http://www.sutel.go.cr/Medios/Descargar/5C448EDAB315A6C1A096E7E6DFF5D02E08E3F4BC

Asamblea Legislativa de la República de Costa Rica. (02 de Mayo de 1978). *Ley Nº 6227; Ley General de la Administración Pública.* Recuperado el 04 de Enero de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=13231&nValor3=90116&param2=1&strTipM=TC&lResultado=2&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (19 de Octubre de 1989). *Ley de la Jurisdicción Constitucional.* Recuperado el 05 de Febrero de 2014, de Sistema Costarricense de Información en Línea: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=38533&nValor3=87797&strTipM=FN

Asamblea Legislativa de la República de Costa Rica. (09 de Agosto de 1994). *Ley Nº 7425 "sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones".* Recuperado el 07 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (28 de Marzo de 1995). *Ley Nº 7486 Aprovación del convenio constitutivo de la Organización Internacional de Telecomunicaciones Marítimas por Satélite (INMARSAT).* Recuperado el 28 de Enero de 2014, de Sistema costarricense de información jurídica en línea: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=18228&nValor3=19451&strTipM=TC

Asamblea Legislativa de la República de Costa Rica. (03 de Noviembre de 1995). *Ley Nº 7558 "Ley Orgánica del Banco Central de Costa Rica".* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=40928&nValor3=93659&param2=1&strTipM=TC&lResultado=6&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (18 de Diciembre de 1995). *Ley Nº 7566 "Creación del sistema de emergencias 9-1-1".* Recuperado el 20 de Febrero de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=39956&nValor3=77883&param2=1&strTipM=TC&lResultado=1&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (05 de Septiembre de 1996). *Ley Nº 7593 de la autoridad reguladora de los servicios públicos.* Recuperado el 11 de Enero de 2014, de Sistema costarricense de información jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=26314&nValor3=80920&param2=1&strTipM=TC&lResultado=3&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (04 de Septiembre de 1996). *Ley Nº 7616 Acuerdo de Cooperación entre Centroamérica y la Comunidad Europea CEE.* Recuperado el 22 de Enero de 2014, de Sistema costarricense de información jurídica en línea: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=29142&nValor3=30816&strTipM=TC

Asamblea Legislativa de la República de Costa Rica. (17 de Diciembre de 1997). *Ley Nº 7732 "Ley Reguladora del Mercado de Valores".* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=29302&nValor3=94261&param2=1&strTipM=TC&lResultado=3&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (18 de Enero de 2000). *Ley Nº 7975 "de Información No Divulgada".* Recuperado el 28 de Marzo de 2014, de Sistema de Información Jurídica en Línea: http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=41810&nValor3=74709&strTipM=TC

Asamblea Legislativa de la República de Costa Rica. (01 de Julio de 2000). *Ley Nº 8302 "Convención de las Naciones Unidas contra la Delincuencia Organizada Trasnacional".* Recuperado el 02 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=50810&nValor3=54705&param2=1&strTipM=TC&lResultado=2&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (16 de Octubre de 2001). *Ley Nº 8131 "de la Administración Financiera de la República y Presupuestos Públicos".* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=47258&nValor3=73503&strTipM=TC

Asamblea Legislativa de la República de Costa Rica. (31 de Mayo de 2002). *Ley Nº 8209 de aprovación del protocolo al Tratado Centroamericano de Telecomunicaciones.* Recuperado el 22 de Enero de 2014, de SUTEL - Normativa internacional: http://www.sutel.go.cr/Medios/Descargar/8A9CDD5671D6A022D34F0443031F1A8236D4DF6C

Asamblea Legislativa de la República de Costa Rica. (17 de Junio de 2003). *Ley Nº 8286 "Acuerdo de cooperación ambiental entre el Gobierno de la República de Costa Rica y el Gobierno de Canadá".* Recuperado el 17 de Febrero de 2014, de Página web de la Secretaría de Planificación Subsectorial de Energía de Costa Rica: http://www.dse.go.cr/es/02ServiciosInfo/Legislacion/PDF/Internacional/Cooperacion/L-8286%20AcuerdoCoop.pdf

Asamblea Legislativa de la República de Costa Rica. (13 de Octubre de 2005). *Ley Nº 8454 "de certificados, firmas digitales y documentos electrónicos".* Recuperado el 02 de Marzo de 2014, de Página web del sistema de firma digital de Costa Rica: http://www.firmadigital.go.cr/Documentos/ley%208454.pdf

Asamblea Legislativa de la República de Costa Rica. (30 de Junio de 2008). Ley Nº 8642 Ley General de Telecomunicaciones. San José , Costa Rica.

Asamblea Legislativa de la República de Costa Rica. (13 de Agosto de 2008). *Ley Nº 8660 de fortalecimiento y modernización de las entidades públicas del sector telecomunicaciones.* Recuperado el 28 de Enero de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63786&nValor3=91177&param2=1&strTipM=TC&lResultado=2&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (22 de Julio de 2009). *Ley Nº 8754 "Ley contra la delincuencia organizada".* Recuperado el 21 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=65903&nValor3=87003&strTipM=TC

Asamblea Legislativa de la República de Costa Rica. (12 de Septiembre de 2011). *Ley Nº 8956 "Ley Reguladora del Contrato de Seguros, reforma Ley Protección al Trabajador, Ley Reguladora Mercado de Seguros y Ley Seguro de Fidelidad".* Recuperado el 16 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=71064&nValor3=86097&param2=1&strTipM=TC&lResultado=2&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (07 de Setiembre de 2011). *Ley Nº 8968 Protección de la persona frente al tratamiento de sus datos personales.* Recuperado el 13 de Marzo de 2014, de Sistema Costarricense de Información Jurídica:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

Asamblea Legislativa de la República de Costa Rica. (03 de Mayo de 2012). *Aprobación del acuerdo entre la República de Costa Ria y el Reino de los Países Bajos para el intercambio de información en materia tributaria y su protocolo.* Recuperado el 09 de Febrero de 2014, de Página web de Deloitte: https://www.deloitte.com/assets/Dcom-CostaRica/Local%20Content/Servicios/Impuestos/Bolet%C3%ADn%20Tributario/2012/120529-cr_tax_Ley9040.pdf

Asamblea Legislativa de la República de Costa Rica. (10 de Julio de 2012). *Ley Nº 9048 "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del título VII del Código Penal".* Recuperado el 17 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&param2=1&strTipM=TC&lResultado=2&strSim=simp

Asamblea Legislativa de la República de Costa Rica. (24 de Abril de 2013). *Ley Nº 9135 "Reforma de los artículos 196, 196 bis, 230, 293 y 295 y adición del artículo 167 bis al Código Penal".* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica en Línea: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74706&nValor3=92348&strTipM=TC

Asamblea Legislativa de la República de Costa Rica. (26 de Agosto de 2013). *Ley Nº 9162 "Expediente digital único de salud".* Recuperado el 14 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=75700&nValor3=93998&param2=1&strTipM=TC&lResultado=1&strSim=simp

Asamblea Nacional Constituyente de la República de Costa Rica. (07 de Noviembre de 1949). *Constitución Política de la República de Costa Rica.* Recuperado el 02 de Agosto de 2013, de Página web de la Organización de Estados Americanos: http://www.oas.org/dil/esp/Constitucion_Costa_Rica.pdf

Autoridad Reguladora de los Servicios Públicos. (06 de Octubre de 2008). *Reglamento de Acceso Universal, Servicio Universal y Solidaridad.* Recuperado el 15 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=64151&nValor3=74276&param2=1&strTipM=TC&lResultado=1&strSim=simp

Autoridad Reguladora de los Servicios Públicos. (18 de Marzo de 2010). *Reglamento Nº 010 "sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones".* Recuperado el 16 de Marzo de 2014, de Sistema Costarricense

de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=67664&nValor3=80265&strTipM=TC

Autoridades Internacionales de Protección de Datos y Privacidad. (14 de Septiembre de 2004). *Resolution on a Draft ISO Privacy Framework Standard.* Recuperado el 12 de Octubre de 2013, de Página web de la 26º Conferencia de las Autoridades Internacionales de Protección de Datos y Privacidad: http://privacyconference2012.org/wps/wcm/connect/c6dc8b804ae898a19bd99ba0fea628d8/2004_W3.pdf?MOD=AJPERES

Autoridades Internacionales de Protección de Datos y Privacidad. (17 de Octubre de 2008). *Draft Resolution on Privacy Protection in Social Network Services.* Recuperado el 12 de Octubre de 2013, de Página web de la 30º Conferencia de las Autoridades Internacionales de Protección de Datos y Privacidad: http://privacyconference2012.org/wps/wcm/connect/8370ed004ae8618d999d99a0fea628d8/2008_E5.pdf?MOD=AJPERES

Autoridades Internacionales de Protección de Datos y Privacidad. (5 de Noviembre de 2009). *International Standards on the Protection of Personal Data and Privacy - The Madrid Resolution.* Recuperado el 11 de Octubre de 2013, de Página web del ministerio de justicia de Israel: http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24464/20091.pdf

Autoridades Internacionales de Protección de Datos y Privacidad. (29 de Octubre de 2010). *Resolution on Privacy by Design.* Recuperado el 12 de Octubre de 2013, de Página web de la 32º Conferencia Internacional de las Autoridades Internacionales de Protección de Datos y Privacidad: http://privacyconference2012.org/wps/wcm/connect/c6a587804adc37639aaf9aa0fea628d8/2010_J5.pdf?MOD=AJPERES

Autoridades Internacionales de Protección de Datos y Privacidad. (26 de Octubre de 2012). *Resolution on cloud computing.* Recuperado el 11 de Octubre de 2013, de Página web de la 34º Conferencia Internacional de Autoridades de Protección de Datos y Privacidad: http://privacyconference2012.org/wps/wcm/connect/92d083804d5dbb9ab90dfbfd6066fd91/Resolutionon_Cloud_Computing.pdf?MOD=AJPERES

Autoridades Internacionales de Protección de Datos y Privacidad. (26 de Octubre de 2012). *Resolution on the future of privacy.* Recuperado el 11 de Octubre de 2013, de Página web de la 34º Conferencia Internacional de Autoridades de Protección de Datos y Privacidad: http://privacyconference2012.org/wps/wcm/connect/ae021f804d5dbfeeb937fbfd6066fd91/aResolution_on_the_Future_of_Privacy.pdf?MOD=AJPERES

Autoridades Internacionales de Protección de Datos y Privacidad. (26 de Octubre de 2012). *Uruguay declaration on profiling.* Recuperado el 11 de Octubre de 2013, de Página

web de la 34º Conferencia Internacional de Autoridades de Protección de Datos y Privacidad: http://privacyconference2012.org/wps/wcm/connect/7b10b0804d5dc38db944fbfd6066fd91/Uruguay_Declaration_final.pdf?MOD=AJPERES

Autoridades Internacionales de Protección de Datos y Privacidad. (24 de Septiembre de 2013). *Declaración de Varsovia sobre la "appification" de la sociedad – La privacidad: una brújula para un mundo en turbulencia.* Recuperado el 11 de Octubre de 2013, de Página web de la 35º Conferencia de Autoridades Internacionales de Protección de Datos y Privacidad: https://privacyconference2013.org/web/pageFiles/kcfinder/files/Declaraci%C3%B3n%20de%20Varsovia.pdf

Ávila Hernández, F., Castaldo, K., & Urdaneta Meza, A. (2007). *Los derechos a la intimidad y a la privacidad en Venezuela y en el derecho comparado.* Recuperado el 16 de Febrero de 2013, de Revista Telemática de Filosofía del Derecho: http://www.rtfd.es/numero11/18-11.pdf

Ax, J. (25 de Abril de 2014). *U.S. judge rules search warrants extend to overseas email accounts.* Recuperado el 03 de Mayo de 2014, de Reuters: http://www.reuters.com/article/2014/04/25/us-usa-tech-warrants-idUSBREA3O24P20140425

Baille, E. (Febrero de 2012). *Derechos de la personalidad en internet.* Recuperado el 16 de Enero de 2013, de Lex-go: http://lexgo.cat/wp-content/uploads/2012/02/Art%C3%ADculo-derechos-de-la-personalidad-e-internet.pdf

BakerHostetler. (20 de Febrero de 2013). *International Compendium of Data Privacy Laws.* Recuperado el 30 de Septiembre de 2013, de Página web de BakerHostetler: http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf

Banco Central de Costa Rica. (21 de Enero de 2014). *Reglamento sobre el Registro Único de Personas Beneficiarias.* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=76646&nValor3=95770&strTipM=TC

Banco Mundial. (2013). *World Development Indicators 2013.* Recuperado el 11 de Enero de 2014, de Página web del Banco Mundial: http://databank.worldbank.org/data/download/WDI-2013-ebook.pdf

Banco Nacional de Costa Rica. (21 de Junio de 2012). *Regulaciones en cuanto a la transferencia de información personal de clientes conforme Ley de protección de la persona frente al tratamiento de sus datos personales .* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72892&nValor3=89234&strTipM=TC

Barett, J. (2002). Customer Data Integration Technology: A Privacy Solution. *The Computer & Internet Lawyer*, 8-11.

Barlow, John Perry. (08 de Febrero de 1996). *Declaración de Independencia del Ciberespacio.* Recuperado el 21 de Marzo de 2014, de BiblioWeb de SinDominio / Página web de la Electronic Frontier Foundation (Documento original): http://biblioweb.sindominio.net/telematica/manif_barlow.html

Barral Viñals, I. (2003). *La protección de los datos personales en internet.* Recuperado el 07 de Abril de 2013, de La regulación del comercio electrónico - vlex.com: http://vlex.com/vid/190219

Barral Viñals, I. (2003). *La regulación del comercio electrónico.* Madrid: Dykinson S.L.

Barreiro, C. (1981). *Derechos Humanos.* Barcelona: Salvat Editores.

Barros Bourie, E. (2013). *Privacidad y honra.* Recuperado el 16 de Febrero de 2013, de vlex.com: http://doctrina.vlex.cl/vid/privacidad-honra-314536282

Battaner, S. (02 de Marzo de 2006). *Intimidad, privacidad y protección de datos de carácter personal.* Recuperado el 04 de Marzo de 2013, de www.baquia.com: http://www.baquia.com/posts/intimidad-privacidad-y-proteccion-de-datos-de-caracter-personal

Bazán, V. (1999). *El Habeas Data, el Derecho a la autodeterminación informativa y la superación del concepto preinformático de la intimidad.* Recuperado el 16 de Marzo de 2013, de Página web de la Biblioteca Jurídica Virtual de la Universidad Nacional Autónoma de México: http://biblio.juridicas.unam.mx/revista/pdf/DerechoComparado/94/art/art1.pdf

Bazán, V. (Julio de 2011). *El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado.* Recuperado el 15 de Marzo de 2013, de vlex.com: http://doctrina.vlex.cl/vid/habeas-autodeterminacion-informativa-43011320

Bazán, V. (2012). *El hábeas data, su autonomía respecto del amparo y la tutela del derecho fundamental de autodeterminación informativa.* Recuperado el 30 de Septiembre de 2013, de Anuario de Derecho Constitucional Latinoamericano: http://www.corteidh.or.cr/tablas/r29666.pdf

Bennett, C. J. (1992). *Regulating Privacy: Data protection and public Policy in Europe and the United States.* Ithaca, New York: Cornell University Press.

Bennett, C., & Raab, C. (2006). *The governance of privacy: Policy instruments in global perspective.* Cambridge: MIT Press.

Berliner Beauftragter für Datenschutz und Informationsfreiheit. (6 de septiembre de 2006). *International Documents on Data Protection in Telecommunications and Media 1983 - 2006.* Recuperado el 01 de abril de 2012, de www.datenschutz-berlin.de: http://www.datenschutz-berlin.de/attachments/334/IWGDPT_WP_brochure.pdf

Bernt, P. (2010). Should the whole world be watching? The tension between social networks and national privacy policies. *38th Research Conference on Communication, Information and Internet Policy* (págs. 1-31). Arlington, Virginia: Social Science Research Network.

Beunen, A. C. (07 de Junio de 2007). *Protection for databases: the European Database Directive and its effects in the Netherlands, France and the United Kingdom.* Recuperado el 13 de Abril de 2013, de Página web del repositorio de la Universidad de Leiden: https://openaccess.leidenuniv.nl/bitstream/handle/1887/12038/02.pdf?sequence=13

Bolaños Chaves, E. A. (2012). *El derecho al olvido en la internet una aplicación a las hemerotecas digitales - Tesis para optar por el grado de licenciatura en Derecho.* Recuperado el 05 de Mayo de 2013, de Página web del Instituto de Investigaciones Jurídicas de la Universidad de Costa Rica: www.iij.ucr.ac.cr/download/file/fid/705

Bond, R. (03 de Junio de 2003). *Data Protection Laws.* Recuperado el 29 de Mayo de 2013, de Página web de Globalcompliance.com: http://www.globalcompliance.com/pdf/data-protection-laws-restrictions.pdf

Boza, B. (2004). *Acceso a la Información del Estado, Marco Legal y Buenas Prácticas.* Recuperado el 10 de Marzo de 2013, de www.ciudadanosaldia.org: http://www.ciudadanosaldia.org/pubs/kas/Libro_Acceso_Informacion.pdf

Bru Cuadrada, E. (Septiembre de 2007). *La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad.* Recuperado el 02 de Febrero de 2013, de Página web de la Universidad Oberta de Cataluñya: www.uoc.edu/idp/5/dt/esp/bru.pdf

Buckert, H. (1982). Institutions of Data Protection: An attempt at a fuctional explanation of European national Data Protection laws. *Computer Law Journal*, 167-188.

Burgoa Orihuela, I. (1996). *Las garantías individuales.* Mexico: Porrúa.

Burkert, H. (1999). *Privacy – Data Protection, A German/European Perspective.* Recuperado el 02 de abril de 2013, de Página Web del Instituto Max PLank para Investigación en Bienes Colectivos: http://www.coll.mpg.de/sites/www.coll.mpg.de/files/text/burkert.pdf

Cámara de Diputados del H. Congreso de la Unión. (14 de Mayo de 1986). *Ley Federal de las Entidades Paraestatales.* Recuperado el 25 de Septiembre de 2013, de Página web del Instituto Federal de Acceso a la Información y Protección de Datos: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/02LFEP.pdf

Cámara de Diputados del H. Congreso de la Unión. (04 de Agosto de 1994). *Ley Federal de Procedimiento Administrativo.* Recuperado el 25 de Septiembre de 2013, de Página web del Instituto Federal de Acceso a la Información y Protección de Datos: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/03LFPA.pdf

Cámara de Diputados del H. Congreso de la Unión. (13 de Marzo de 2002). *Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.* Recuperado el 25 de Septiembre de 2013, de Página web del Instituto Federal de Acceso a la Información y Protección de Datos: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/4LFRASP.pdf

Cámara de Diputados del H. Congreso de la Unión. (11 de Junio de 2002). *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.* Recuperado el 25 de Septiembre de 2013, de Página web del Instituto Federal de Acceso a la Información y Protección de Datos: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/05LFTAIPG.pdf

Cámara de Diputados del H. Congreso de la Unión. (05 de Julio de 2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Recuperado el 25 de Septiembre de 2013, de Página web del Instituto Federal de Acceso a la Información y Protección de Datos: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/06LFPDPPP.pdf

Campbell, M., Giay, G., & Peruzzotti, M. (Marzo de 2012). *Argentina.* Recuperado el 06 de Septiembre de 2013, de DLA Piper's Data Protection Laws of the World: http://www.edrm.net/resources/data-privacy-protection/data-protection-laws/argentina

Canadian Standards Association. (Marzo de 1996). *Model Code for the Protection of Personal Information.* Recuperado el 15 de Abril de 2014, de Simson.net: http://simson.net/ref/RSA/1996.CanadianStandardsAssociation.ModelCodeForProtectionOfPersonalInfo.pdf

Carrión, H. (30 de Enero de 2013). *La sociedad de la información - Tecnologas de información y comunicaciones.* Recuperado el 05 de Febrero de 2013, de Centro de Investigación para la Sociedad de la Información: http://www.imaginar.org/docs/sociedad_informacion_wikipedia.pdf

Carter, L. G., & Miyata, M. (01 de Junio de 2012). *Data Protection in Japan: overview.* Recuperado el 04 de Octubre de 2013, de Practical law, a Thomson Reuters legal solution: http://uk.practicallaw.com/5-520-1289

Carvajal Pérez, M. (09 de Julio de 2003). *Transparencia judicial y protección de datos personales. Dos valores complementarios.* Recuperado el 09 de Marzo de 2014, de Seminario-Taller Internet y Sistema Judicial en América Latina y el Caribe: http://www.iijusticia.org/heredia/PDF/Carvajal%20Perez.pdf

Carvajal Pérez, M. (Viernes de Septiembre de 2013). *El Hábeas Data y la protección de los datos personales. Perspectivas y retos de su manejo.* Recuperado el 02 de Marzo de 2014, de Seminario Libertad de Información y Datos Personales: http://www.youtube.com/watch?v=wlkVbsFl3NY

Carvajal Pérez, M. (09 de Marzo de 2014). Sobre las etapas en el tratamiento histórico jurisprudencial de la Protección de Datos Personales en Costa Rica. (A. Quesada Rodríguez, Entrevistador)

Castán Tobeñas, J. (1952). *Derechos de la personalidad.* Madrid: Reus.

Castillo Jiménez, C. (2001). *Protección del derecho a la intimidad y las nuevas tecnologas de la información.* Recuperado el 16 de Febrero de 2013, de Página web de la Universidad de Huelva: http://www.uhu.es/derechoyconocimiento/DyC01/A02.pdf

Cavoukian, A. (Febrero de 2001). *Privacy by Design - Los 7 principios fundamentales.* Recuperado el 29 de Abril de 2014, de Página web de PbD: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf

Cavoukian, A. (Julio de 2013). *A primer on metadata: separating fact from fiction.* Recuperado el 01 de Abril de 2014, de Privacy by Design Canada: http://www.privacybydesign.ca/content/uploads/2013/07/Metadata.pdf

Center for Democracy & Technology. (2013). *Security and Surveillannce.* Recuperado el 05 de Agosto de 2013, de Center for Democracy & Technology: https://www.cdt.org/issue/wiretap-ecpa

Centro de las Naciones Unidas sobre Corporaciones Transnacionales. (1982). *Transnational corporations and transborder data flows: a technical paper.* Recuperado el 20 de Mayo de 2013, de Página web del Centro de las Naciones Unidas sobre Corporaciones Transnacionales: http://unctc.unctad.org/data/e82iia4a.pdf

Charles Raul, A. (1 de Octubre de 2010). *www.sidley.com.* Recuperado el 15 de Febrero de 2012, de Where are we on locational privacy?: http://www.sidley.com/files/RepresentativeExperience/005cdd76-9f4d-4237-bf77-4f6985f38025/Presentation/ceRepExperienceDocument1/Where%20Are%20We%20on%20Locational%20Privacy.pdf

Chaves Zúñiga, C. (2009). *La protección de datos del trabajador frente a las posibilidades de control del empleador, Trabajo final de graduación para optar por el grado de Licenciatura en Derecho.* San José: Universidad de Costa Rica.

Chinchilla Sandí, C. (2005). Personalidad virtual: necesidad de una reforma constitucional. *Revista de Derecho y Tecnologías de la información*(3), 1-11.

Chirino, A. (1997). *Autodeterminación informativa y estado de derecho en la sociedad tecnológica.* San José: CONAMAJ.

Chirino, A. (1997). *El "habeas data" como realización del derecho a la autodeterminación informativa. Ideas en torno a un proyecto e ley.* San José: Asamblea Legislativa.

Chirino, A. (1997). *La protección constitucional de la intimidad.* San José: UNED.

Chirino, A. (1997). *La protección de la autodeterminación informativa como un nuevo bien jurídico penalmente tutelado.* Buenos Aires: Editores Del Puerto.

Chirino, A. (1997). *Tecnología de la información y proceso penal. Análisis de una crisis anunciada.* San José: UNED.

Chirino, A. (2008). Seguridad ciudadana y prevención del delito. Retos de la protección de datos ante las necesidades de seguridad. *IUS DOCTRINA, 1*(2), 1-39.

Chirino, A. (01 de Agosto de 2011). *El derecho a la intimidad en Costa Rica.* Recuperado el 21 de Febrero de 2012, de OPENCOURSEWARE UNED COSTA RICA Sistema de Estudios de Posgrado Tecnología y Trabajo: http://www.ocw.uned.ac.cr/eduCommons/s.e.p/tecnologia-y-trabajo/recursos/descargar-curso-completo/view

Chirino, A., & Carvajal, M. (01 de Agosto de 2005). El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica. *Protección de datos de carácter personal en Iberoamérica: (II Encuentro Iberoamericano de Protección de Datos)* (págs. 197-260). La Antigua-Guatemala: Tirant Lo Blanch.

Colegio de Periodistas de Costa Rica. (16 de Agosto de 2011). *Código de ética de las y los profesionales en comunicación.* Recuperado el 16 de Marzo de 2014, de Página web del Colegio de Periodistas de Costa Rica: http://www.colper.or.cr/userfiles/file/juridico/codigos/codigo_etica.pdf

Comisión de las Comunidades Europeas. (1997). *Comunicación de la Comisión de las Comunidades Europeas, al Parlamento Europeo, al Comité económico social y al Comité de las Regiones sobre Iniciativa europea de Comercio Electrónico [COM (97) 157 final].* Bruselas: Comisión de las Comunidades Europeas.

Comisión de Reforma a la Ley Australiana. (2013). *Collection - Unsolicited Personal Information*. Recuperado el 13 de Octubre de 2013, de Página web del Gobierno de Australia: http://www.alrc.gov.au/publications/21.%20Collection/unsolicited-personal-information

Comisión Europea. (1997). *Green Paper on the convergence of telecommunications, media and information technology sectors, and the implications for regulation.* Bruselas: Comisión Europea.

Comisión Europea. (25 de Agosto de 2000). *Commision decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adecuacy of the protection provided by the safe harbour privacy principles.* Recuperado el 06 de

Noviembre de 2013, de EURLex: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

Comisión Europea. (2000). *Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos.* Bruselas: Comisión Europea.

Comisión Europea. (20 de Diciembre de 2001). *2002/2/EC: Commission Decision on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act.* Recuperado el 15 de Abril de 2014, de Página web de la Biblioteca Legislativa de la Unión Europea: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002D0002

Comisión Europea. (30 de Junio de 2003). *Commission decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina.* Recuperado el 04 de Agosto de 2013, de Página web de la Comisión Europea.

Comisión Europea. (2007). *Towards a New Framework for Electronic Communications infrastructure and associated services, The 1999 Communications Review".* Recuperado el 20 de 05 de 2011, de la Página Web de la Comisión Europea: http://ec.europa.eu/comm/information_society/policy/telecom/review99/pdf/review_en.pdf

Comisión Europea. (25 de Enero de 2012). *Propuesta de Directiva 2012/0010(COD).* Recuperado el 15 de Junio de 2013, de Página web oficial de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:ES:PDF

Comisión Europea. (25 de Enero de 2012). *Propuesta de Reglamento General de Protección de Datos 2012/0011(COD).* Recuperado el 15 de Junio de 2013, de Comisión Europea - Página web oficial de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

Comisión Europea. (2013). *Legislation*. Recuperado el 01 de Septiembre de 2013, de Página web de la Comisión Europea: http://ec.europa.eu/justice/data-protection/law/index_en.htm

Comisión Europea. (2014). *Article 29 Working Party.* Recuperado el 22 de Julio de 2014, de Página web de la Comisión Europea: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

Comisión Europea. (08 de Abril de 2014). *Frequently Asked Questions: The Data Retention Directive.* Recuperado el 14 de Abril de 2014, de European Commission: Press Releases Database: http://europa.eu/rapid/press-release_MEMO-14-269_en.htm

Comunidad Europea y Gobiernos Centroamericanos. (15 de Diciembre de 2003). *Acuerdo de diálogo político y cooperación entre la Comunidad Europea y sus estados miembros, por una parte,y las Repúblicas de Costa Rica, El Salvador, Guatemala, Honduras,*

*Nicaragua y Panamá, por otra parte.* Recuperado el 08 de Febrero de 2014, de European external action service: http://eeas.europa.eu/ca/pol/pdca_12_03_es.pdf

Conde Ortiz, C. (2005). *La protección de datos personales.* Recuperado el 01 de Diciembre de 2012, de vlex.com: http://libros-revistas-derecho.vlex.es/source/proteccion-datos-personales-1247

Congreso Constituyente de México. (05 de febrero de 1917). *Constitución Política de los Estados Unidos Mexicanos.* Recuperado el 21 de Septiembre de 2013, de Página web de la Cámara de Diputados del H. Congreso de la Unión Mexicana: http://www.diputados.gob.mx/LeyesBiblio/pdf/1.pdf

Congreso Constituyente Democrático del Perú. (1993). *Constitución Política del Perú.* Recuperado el 06 de Septiembre de 2013, de Página web del Tribunal Constitucional Peruano: www.tc.gob.pe/legconperu/constitucion.html

Congreso de la Nación Argentina. (30 de Octubre de 2000). *Ley de Protección de los Datos Personales - Ley 25.326.* Recuperado el 30 de Septiembre de 2013, de Página Web del Ministerio de Economía y Finanzas Públicas: http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

Congreso de la República de Colombia. (31 de Diciembre de 2008). *Ley Estatutaria 1266 de 2008.* Recuperado el 30 de Septiembre de 2013, de Página web de la Secretaría General del Senado: http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html

Congreso de la República de Colombia. (05 de Enero de 2009). *Ley Nº 1273.* Recuperado el 21 de Marzo de 2014, de Página web del Ministerio de Tecnologías de la Información y la Comunicación de Colombia: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Congreso de la República de Colombia. (17 de Octubre de 2012). *Ley Estatutaria 1581 de 2012.* Recuperado el 30 de Septiembre de 2012, de Página web de la Alcaldía de Bogotá: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Congreso de la República de Colombia. (17 de Abril de 2013). *Ley Estatutaria 1621 de 2013.* Recuperado el 26 de Marzo de 2014, de Página web de la Presidencia de la República de Colombia: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/2013/LEY%201621%20DEL%2017%20DE%20ABRIL%20DE%202013.pdf

Congreso de la República del Perú. (31 de Mayo de 2004). *Código Procesal Constitucional - Ley Nº 28237.* Recuperado el 06 de Septiembre de 2013, de Página web del Tribunal Constitucional de la República del Perú: http://tc.gob.pe/Codigo_Procesal.html

Congreso de la República del Perú. (2011). *Ley de Protección de Datos Personales - Nº 29733.* Recuperado el 06 de Septiembre de 2013, de Página web del Congreso de la República del Perú:

http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc01_2011.nsf/d99575da99ebfbe305256f2e006d1cf0/a06f4a0ad466b8b305257a060074e4c1/$FILE/29733.pdf

Congreso de los Diputados. (13 de Diciembre de 1999). *Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.* Recuperado el 03 de Octubre de 2013, de Página web de la Universidad de Alicante: http://www.ua.es/es/normativa/datospersonales/pdfs/Ley15_99.pdf

Congreso de los Estados Unidos de América. (1938). *Federal trade Commision Act of 1938.* Recuperado el 06 de Agosto de 2013, de Legal Information Institute - Cornell University Law School: http://www.law.cornell.edu/uscode/text/15/41

Congreso de los Estados Unidos de América. (1966). *Freedom of Information Act of 1966.* Recuperado el 28 de Agosto de 2013, de Página web del Departamento de Justicia de los Estados Unidos de América: http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm

Congreso de los Estados Unidos de América. (1970). *Bank Secrecy Act of 1970*. Recuperado el 03 de Agosto de 2013, de Financial Crimes Enforcement Network - United States Department of the Treasury: http://www.fincen.gov/statutes_regs/bsa/

Congreso de los Estados Unidos de América. (26 de Octubre de 1970). *Fair Credit Reporting Act.* Recuperado el 06 de Agosto de 2013, de Página web de la Federal Trade Commision: http://www.ftc.gov/os/statutes/fcradoc.pdf

Congreso de los Estados Unidos de América. (1974). *Equal Credit Oportuunity Act of 1974*. Recuperado el 06 de Agosto de 2013, de Legal Information Institute - Cornell university Law School: http://www.law.cornell.edu/uscode/text/15/1691

Congreso de los Estados Unidos de América. (1974). *Family Education Rights and Privacy Acts of 1974.* Recuperado el 06 de Agosto de 2013, de Página web del Electronic Pivacy Informattion Center: https://epic.org/privacy/education/ferpa.html

Congreso de los Estados Unidos de América. (31 de Diciembre de 1974). *Privacy Act of 1974*. Recuperado el 06 de Agosto de 2013, de Página web del Departamento de Justicia de los Estados Unidos de América: http://www.justice.gov/opcl/privstat.htm

Congreso de los Estados Unidos de América. (1978). *Electronic Funds Transfer Act of 1978*. Recuperado el 06 de Agosto de 2013, de Federal deposit Insurance Corporation - FDIC Law, Regulations, Related Acts: http://www.fdic.gov/regulations/laws/rules/6500-1350.html

Congreso de los Estados Unidos de América. (1978). *Fair Debt Collection Practices Act of 1996.* Recuperado el 06 de Agosto de 2013, de Página web de la Federal Trade Commission: http://www.ftc.gov/os/statutes/fdcpa/fdcpact.shtm

Congreso de los Estados Unidos de América. (1978). *Right to Financial Privacy Act of 1978.* Recuperado el 29 de Agosto de 2013, de Access Reports: http://www.accessreports.com/statutes/RFPA.htm

Congreso de los Estados Unidos de América. (1980). *Privacy Protection Act of 1980*. Recuperado el 06 de Agosto de 2013, de Legal Information Institute - Cornell University Law School: http://www.law.cornell.edu/uscode/text/42/2000aa

Congreso de los Estados Unidos de América. (1984). *47 USC § 551 - Protection of subscriber privacy*. Recuperado el 03 de Agosto de 2013, de Legal Information Institute - Corenell University Law School: http://www.law.cornell.edu/uscode/text/47/551

Congreso de los Estados Unidos de América. (1984). *Computer Fraud and Abuse Act of 1984*. Recuperado el 03 de Agosto de 2013, de Legal Information Insitute - Cornell University Law School: http://www.law.cornell.edu/uscode/text/18/1030

Congreso de los Estados Unidos de América. (1984). *Electronic Communications Privacy Act of 1984.* Recuperado el 05 de Agosto de 2013, de Legal Information Institute - Cornell University Law School: http://www.law.cornell.edu/uscode/text/18/2510

Congreso de los Estados Unidos de América. (1988). *Computer Matching and Privacy Protection Act of 1988*. Recuperado el 04 de Agosto de 2013, de Legal Information Institute - Conell University Law School: http://www.law.cornell.edu/uscode/text/5/552a

Congreso de los Estados Unidos de América. (1988). *Video Privacy Protection Act of 1988*. Recuperado el 06 de Agosto de 2013, de Legal Information Institute - Corrnell university Law School: http://www.law.cornell.edu/uscode/text/18/2710

Congreso de los Estados Unidos de América. (1990). *Americans with Disabilities Act of 1990*. Recuperado el 03 de Agosto de 2013, de U.S. Equal Employment Opportunity Commission: http://www.eeoc.gov/laws/statutes/ada.cfm

Congreso de los Estados Unidos de América. (1991). *Telephone Consumer Protection Act of 1991.* Recuperado el 22 de Agosto de 2013, de Legal Information Institute - Cornell University Law School: http://www.law.cornell.edu/uscode/text/47/227

Congreso de los Estados Unidos de América. (1994). *Communications Assistance for Law Enforcement Act of 1994*. Recuperado el 04 de Agosto de 2013, de Electronic Privacy Information Center: https://epic.org/privacy/wiretap/calea/calea_law.html

Congreso de los Estados Unidos de América. (1994). *Drivers Privacy Protection Act of 1994.* Recuperado el 05 de Agostto de 2013, de Legal Information Institute - Cornell University Law School: http://www.law.cornell.edu/uscode/text/18/2721

Congreso de los Estados Unidos de América. (03 de Enero de 1996). *Electronic Freedom of Information Act.* Recuperado el 06 de Agosto de 2013, de U.S. Government Printing

Office: http://www.gpo.gov/fdsys/pkg/BILLS-104hr3802enr/pdf/BILLS-104hr3802enr.pdf

Congreso de los Estados Unidos de América. (1996). *Fair Credit Reporting Act &Consumer Credit Reporting Reform Act of 1996.* Recuperado el 03 de Agosto de 2013, de federal Trade Commision: http://www.ftc.gov/os/statutes/031224fcra.pdf

Congreso de los Estados Unidos de América. (1996). *Health Insurance Porability and Accountability Act of 1996.* Recuperado el 06 de Agosto de 2013, de U.S. Government Printing Office: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

Congreso de los Estados Unidos de América. (1996). *Telecommunications Act of 1996.* Recuperado el 07 de Agosto de 2013, de Página web de la FCC: http://transition.fcc.gov/Reports/tcom1996.pdf

Congreso de los Estados Unidos de América. (21 de Octubre de 1998). *Children's Online Privacy Protection Act of 1998*. Recuperado el 06 de Agosto de 2013, de Página web de la Federal Trade Commission: http://www.ftc.gov/ogc/coppa1.htm

Congreso de los Estados Unidos de América. (30 de Octubre de 1998). *Identity Theft and Assumption Deterrence Act of 1998*. Recuperado el 06 de Agosto de 2013, de Página web de la Federal trade Commision: http://www.ftc.gov/os/statutes/itada/itadact.htm

Congreso de los Estados Unidos de América. (1999). *Gramm-Leach-Bliley Financial Modernization Act of 1999.* Recuperado el 06 de Agosto de 2013, de U.S. Government Printing Office: http://www.gpo.gov/fdsys/pkg/BILLS-106s900enr/pdf/BILLS-106s900enr.pdf

Congreso de los Estados Unidos de América. (21 de Diciembre de 2000). *Children's Internet Protection Act of 2000*. Recuperado el 06 de Agosto de 2013, de Página web de la Federal Communications Commision: http://ifea.net/cipa.pdf

Congreso de los Estados Unidos de América. (26 de Octubre de 2001). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.* Recuperado el 07 de Agosto de 2013, de U.S. Government Printing Office: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

Congreso de los Estados Unidos de América. (30 de Julio de 2002). *Sarbanes-Oxley Act of 2002.* Recuperado el 07 de Agosto de 2013, de University of Cincinnati - College of Law: http://taft.law.uc.edu/CCL/SOact/soact.pdf

Congreso de los Estados Unidos de América. (04 de Diciembre de 2003). *Fair and Accurate Credit Transactions Act of 2003.* Recuperado el 06 de Agosto de 2013, de U.S. Government Printing Office: http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf

Congreso de los Estados Unidos de América. (01 de Junio de 2005). *Disposal of Consumer Report Information and Records, Final Rule.* Recuperado el 06 de Agosto de 2013, de Página web de la Federal Trade Commision: http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf

Congreso de los Estados Unidos de América. (03 de Octubre de 2006). *Financial Services Regulatory Relief Act of 2006*. Recuperado el 06 de Agosto de 2013, de Página web de gobtrack.us: http://www.govtrack.us/congress/bills/109/s2856/text

Congreso de los Estados Unidos de América. (2009 de Febrero de 2009). *Healtth Information Technology for Economic and Clinical Health Act of 2009.* Recuperado el 06 de Agosto de 2013, de U.S. Department of Health & Human Services: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

Congreso General Constituyente de la Nación Argentina. (03 de Enero de 1995). *Constitución Política de la Nación Argentina.* Recuperado el 06 de Septiembre de 2013, de Página web del Ministerio de Economía y Finanzas Públicas de Argentina: http://infoleg.mecon.gov.ar/infolegInternet/anexos/0-4999/804/norma.htm

Congreso Nacional Brasileño. (25 de Marzo de 2014). *Subemenda substitutiva global às emendas de plenario ao projeto de lei Nº 2.126 de 2011.* Recuperado el 25 de Marzo de 2014, de Página web de la cámara de diputados: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1238705&filename=Tramitacao-PL+2126/2011

Consejo de Europa. (04 de Noviembre de 1950). *Convención Europea de Derechos Humanos.* Recuperado el 04 de Marzo de 2013, de Página web de la Corte Europea de Derechos Humanos: http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/Convention_SPA.pdf

Consejo de Europa. (1968). *Recomendación 509 - Human rights and modern scientifica and technological developments.* Recuperado el 16 de Abril de 2013, de Página web de la Asamblea Parlamentaria del Coonsejo de Europa: http://www.assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=14546&Language=EN

Consejo de Europa. (28 de Enero de 1981). *Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.* Recuperado el 06 de Mayo de 2013, de Página web del Consejo de Europa: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Consejo de Europa. (08 de Noviembre de 2001). *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.* Recuperado el 13 de Junio de 2013, de Página web del Consejo de Europa: http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm

Consejo de la Unión Europea. (27 de Noviembre de 2008). *Decisión Marco 2008/977/JAI.* Recuperado el 15 de Junio de 2013, de Diario oficial de la Unión Europea - Página web oficial de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:es:PDF

Consumer Financial Protection Bureau. (Enero de 2013). *A Summary of Your Rights Under the Fair Credit Reporting Act.* Recuperado el 27 de Agosto de 2013, de Página web del Pomona College: http://www.pomona.edu/administration/human-resources/employment/fair-credit-report-rights-summary.pdf

Contraloría General de la República. (31 de Julio de 2007). *"Normas técnicas para la gestión y el control de las Tecnologías de Información" (N-2-2007-CO-DFOE).* Recuperado el 01 de Mayo de 2014, de Página web de la Contraloría Universitaria de la Universidad de Costa Rica: http://www.ocu.ucr.ac.cr/RIDS/N-2-2007-CO-DFOENormasGestionControlTI-CGR.pdf

Convención Nacional Constituyente de Paraguay. (20 de junio de 1992). *Constitución Política de la República del Paraguay.* Recuperado el 03 de Septiembre de 2013, de constitution.org: http://www.constitution.org/cons/paraguay.htm

Cordero Sancho, M. (30 de Junio de 2013). *Aporte de las telecomunicaciones al PIB de Costa Rica ha crecido un 45% en cinco años.* Recuperado el 23 de Enero de 2014, de El Financiero: http://www.elfinancierocr.com/tecnologia/Cinco_anos_de_la_apertura_del_mercado_de_Telecomunicaciones-telefonia_movil-Internet_movil-Claro-ICE-Movistar_0_326367385.html

Córdoba Ortega, J. (1996). El libre acceso a los departamentos administrativos y el Secreto de Estado. *Ivstitia Nº 114-115*, 29-35.

Córdoba Ortega, J. (2004). *La Legislación Costarricense y el Derecho de Acceso a la Información Pública: Un Estudio Actual.* Recuperado el 10 de Mayo de 2013, de Página web del Instituto de Investigaciones Jurídicas de la Facultad de Derecho de la Universidad de Costa Rica: http://www.iij.ucr.ac.cr/archivos/publicaciones/libros/Legislacion%20costarricense%20y%20derecho%20de%20acceso%20a%20la%20informacion%20publica.pdf

Corrales Castillo, W. (2011). *Viabilidad jurídica de la implementación del recurso de habeas data para regular la discriminación en los procesos de selección de personal en razón de bases de datos. Trabajo final de graduación para optar por el grado de licenciatura en Derecho.* San José: Universidad de Costa Rica.

Corripio Gil-Delgado, M. d. (2001). *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en internet.* Barcelona: Editorial vLex.

Corte de Justicia de la Unión Europea. (08 de Abril de 2014). *Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others - Press Release.*

Recuperado el 14 de Abril de 2014, de Página web de la Corte de Justicia de la Unión Europea: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Costa, J. C. (Septiembre de 2008). *La condición de la persona en Roma y los Derechos Humanos.* Recuperado el 27 de enero de 2013, de AEQUITAS VIRTUAL Publicación de la facultad de Ciencias Jurídicas, Universidad del Salvador, República Argentina. Número 7: http://www.salvador.edu.ar/juri/aequitasNE/nrosiete/Derecho%20Romano.pdf

Cruz Ayala, C. G. (Agosto de 2010). Protección de datos personales en posesión de particulares. *Revista El Mundo del Abogado*(136), 23-26.

Davara Rodríguez, M. Á. (Octubre de 2006). *Guía práctica de protección de datos para ayuntamientos.* Recuperado el 16 de Abril de 2013, de Google Books: http://books.google.co.cr/books?id=bxarMdtSEsoC

De Abreau Dallari, D. (1997). *El Hábeas Data en Brasil.* Recuperado el 03 de Septiembre de 2013, de Ius et Praxis - Red de Revistas Científicas de América Latina, el Caribe, España y Portugal: http://www.redalyc.org/artículo.oa?id=19730108

De la Parra Trujillo, E. (2001). *Los derechos de la personalidad: Teoría general y su distinción con los derechos humanos y las garantías individuales.* Recuperado el 09 de Enero de 2013, de Biblioteca Jurídica Virtual, UNAM: http://www.juridicas.unam.mx/publica/librev/rev/jurid/cont/31/pr/pr10.pdf

De Lama Aymá, A. (2004). *La protección de los Derechos de la Personalidad del Menor de Edad - Tesis Doctoral.* Recuperado el 05 de enero de 2013, de Sitio Web de la Universidad Autónoma de Barcelona: http://hdl.handle.net/10803/5207

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (25 de Marzo de 2013). *Unique in the Crowd: The privacy bounds of human mobility.* Recuperado el 18 de Mayo de 2013, de Scientific Reports - Revista Nature: http://www.nature.com/srep/2013/130325/srep01376/pdf/srep01376.pdf

de Quinto Zumárraga, F. (2002). *Los componentes de la seguridad en un entorno TIC'S.* Recuperado el 11 de Abril de 2013, de Protección informática y legal de datos personales - vlex.com: http://libros-revistas-derecho.vlex.es/vid/componentes-seguridad-entorno-tic-s-182442

De Theramond, G. F. (1994). *Interconexión de Costa Rica a las Grandes Redes de Investigación Bitnet e Internet.* Recuperado el 22 de Enero de 2014, de Ideario de la Ciencia y la Tecnología: Hacia el Nuevo Milenio: http://asterix.crnet.cr/gdt/InterconexionCR.pdf

Departamento de Estado de los Estados Unidos de América. (03 de Noviembre de 2003). *Case No. 200301593 - Segment No. SANJO001.* Recuperado el 23 de Mayo de 2013, de Página web de Epic.org: http://epic.org/privacy/choicepoint/cpdos11.3.03.pdf

Departamento de Transporte de Estados Unidos. (Agosto de 2001). *File: Hierarchical Model.svg.* Recuperado el 01 de Junio de 2014, de Wikimedia Commons: http://upload.wikimedia.org/wikipedia/commons/thumb/e/eb/Hierarchical_Model.svg/548px-Hierarchical_Model.svg.png

Departamento de Transporte de Estados Unidos. (Agosto de 2001). *File: Relational Model.svg.* Recuperado el 01 de Junio de 2014, de Wikimedia Commons: http://upload.wikimedia.org/wikipedia/commons/thumb/d/da/Relational_Model.svg/543px-Relational_Model.svg.png

Determann, L., & Hwang, J. D. (Setiembre de 2009). Data Security Requirements Evolve: From Reasonableness to Specifics. *The Computer and Internet Lawyer, 26*(9), 6-26.

Días Cafferata, S. (2009). El Derecho de Acceso a la Información Pública: Situación Actual y Propuestas para una Ley. *Lecciones y Ensayos, nro. 86.*, 151-185.

Diebold, J. (1974). *El hombre y el ordenador.* Madrid: Pirámide.

Dietrich Plaza, C. (2007). *El tratado de Prüm en el marco de la regulación de la protección de datos personales en la Unión Europea.* Recuperado el 27 de Mayo de 2013, de Dialnet - Revista de derecho constitucional europeo: http://dialnet.unirioja.es/descarga/articulo/2492890.pdf

Diffie, W., & Landau, S. (1998). *Privacy on the line: The politics of wiretapping and encryption.* Cambridge: MIT Press.

Dirección Nacional de Protección de los Datos Personales. (22 de Septiembre de 2006). *Protección de los Datos Personales - Medidas de seguridad para el tratamiento y conservación de los datos personales en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados.* Recuperado el 06 de Septiembre de 2013, de protección de datos: http://www.protecciondedatos.com.ar/disp112006.htm

Domínguez Guillén, M. C. (2003). *Sobre los derechos de la personalidad.* Recuperado el 05 de enero de 2013, de Dialnet - Díkaion, Revista de actualidad jurídica: http://dialnet.unirioja.es/descarga/articulo/2107639.pdf

Dromi, R. (2008). *Telecomunicaciones, interconección y convergencia tecnológica.* Buenos Aires: Ciudad Argentina.

Duri, S., Eliott, J., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., y otros. (2004). Data Protection and Data Sharing in Telematics. *Mobile Networks and Applications*, 1-22.

Dwoskin, E. (28 de Octubre de 2013). *Web giants threathen end to Cookie tracking.* Recuperado el 05 de Noviembre de 2013, de The wall street journal: http://m.us.wsj.com/articles/SB10001424052702304682504579157780178992984?mobile=y

Editorial Revista Hospitales de Costa Rica. (Enero de 1997). *Reseña histórica de las Insituciones del Sector Salud.* Recuperado el 23 de Enero de 2014, de Biblioteca Nacional de Salud y Seguridad Social - Revista Hospitales de Costa Rica: http://www.binasss.sa.cr/revistas/hospitales/art84

Electronic Frontier Foundation. (2013). *CALEA - The perils of wiretapping the Internet*. Recuperado el 04 de Agosto de 2013, de Página web de la EFF: https://www.eff.org/issues/calea

Electronic Privacy Information Center. (2013). *Council of Europe Privacy Convention.* Recuperado el 05 de Octubre de 2013, de Página web de EPIC.org: http://epic.org/privacy/intl/coeconvention/

Electronic Privacy Information Center. (11 de Marzo de 2013). *Freedom of Information Gallery 2013*. Recuperado el 12 de Marzo de 2013, de Página web de epic.org: http://epic.org/foiagallery2013.html

Electronic Privacy Information Center. (2013). *The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record.* Recuperado el 05 de Agosto de 2013, de epic.org: https://epic.org/privacy/drivers/

Electronic Privacy Information Center. (2013). *The Privacy Act of 1974.* Recuperado el 19 de Agosto de 2013, de Página web del Electronic Privacy Information Center: http://epic.org/privacy/1974act/

Electronic Privacy Information Center. (2013). *Video Privacy Protection Act.* Recuperado el 30 de Agosto de 2013, de Página web de EPIC: http://epic.org/privacy/vppa/

Encabo Vera, M. (2012). *Derechos de la Personalidad.* Recuperado el 03 de Febrero de 2013, de Página web de la Editorial Marcial Pons: http://www.marcialpons.es/static/pdf/9788497689687.pdf

EPIC.org. (14 de Agosto de 2002). *U.S. Department of Defense Requisition Order Citizen Prices.* Recuperado el 23 de Mayo de 2013, de Página web de epic.org: http://epic.org/privacy/publicrecords/citizenprices.pdf

Epic.org. (11 de Junio de 2011). *In re Facebook and the Facial Identification of Users.* Recuperado el 27 de Marzo de 2014, de Página web de epic.org: http://epic.org/privacy/facebook/facebook_and_facial_recognitio.html#summary

EU network of independent experts on fundamental rights. (Junio de 2006). *Commentary of the charter of fundamental rights of the European Union.* Recuperado el 06 de Junio de 2013, de Página web de la Comisión Europea: http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf

Facultad de Derecho de la Universidad de Málaga. (2007). *Enciclopedia y Biblioteca Virtual de las Ciencias Sociales, Económicas y Jurídicas.* Recuperado el 05 de enero de 2013, de

eumed.net - Facultad de Derecho de la Universidad de Málaga: http://www.eumed.net/cursecon/dic/dent/d/dep.htm

Federal Communications Commision. (2013). *Children's Internet Protection Act Guide*. Recuperado el 7 de Agosto de 2013, de Página web de la FCC: https://www.fcc.gov/guides/childrens-internet-protection-act

Federal Communications Commision. (8 de Enero de 2013). *Communications Assistance for Law Enforcement Act*. Recuperado el 04 de Agosto de 2013, de FCC Encyclopedia: https://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act

Fernández Burgueño, P. (17 de Septiembre de 2011). *Aspectos jurídicos de la identidad digital y la reputación online.* Recuperado el 05 de Febrero de 2013, de Página web de la Universitat Jaume I: http://repositori.uji.es/xmlui/bitstream/handle/10234/43024/Pablo%20Fern%C3%A1ndez%20Burgue%C3%B1o.pdf?sequence=1

Ferrajoli, L. (2004). *Derechos y garantas, la ley del más débil.* Madrid: Trotta.

Ferrajoli, L. (Julio de 2006). *Sobre los Derechos Fundamentales.* Recuperado el 06 de Febrero de 2013, de Página web de la Universidad Nacional Autónoma de México: http://www.ejournal.unam.mx/cuc/cconst15/CUC1505.pdf

Flores Dapkevicius, R. R. (23 de Septiembre de 2005). *El habeas data en Uruguay y Argentina.* Recuperado el 2013 de Septiembre de 2013, de Âmbito Jurídico: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=271

Foro de Cooperación Económica Asia-Pacífico. (2005). *APEC cross-border privacy rules system program requirements.* Recuperado el 23 de Marzo de 2014, de Página web de APEC: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-ProgramRequirements.ashx

Foro de Cooperación Económica Asia-Pacífico. (2005). *APEC Privacy Framework.* Recuperado el 10 de Octubre de 2013, de Página web de la APEC: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Galindo Garfias, I. (1995). *Derecho Civil.* Mexico: Porrua.

García Aguilar, N. (s.f.). *La protección de los datos personales en la prestación de nuevos servicios de telecomunicaciones.* Recuperado el 8 de Septiembre de 2011, de Revista de derecho vLex: http://libros-revistas-derecho.vlex.es/vid/prestacion-nuevos-telecomunicaciones-118213

García Fernández, D. (Junio de 2002). *La persona y su derecho a la intimidad .* Recuperado el 16 de Febrero de 2013, de vlex.com: http://doctrina.vlex.com.mx/vid/persona-derecho-intimidad-54072682

García P, G., & Contreras V, P. (s.f.). *Derecho de acceso a la información en Chile: Nueva Regulación e Implicancias para el Sector de la Defensa Nacional.* Recuperado el 10 de Mayo de 2013, de 2009: http://www.scielo.cl/pdf/estconst/v7n1/art05.pdf

García, T. (1991). *Apuntes de Introducción al Estudio del Derecho.* México: Porrua.

Garriga Domínguez, A. (2009). *El derecho a al autodeterminación informativa. Acuerdos y desacuerdos con la doctrina del tribunal constitucional.* Recuperado el 15 de Marzo de 2013, de vlex.com: vlex.com/vid/autodeterminacion-informativa-desacuerdos-69947566

Garriga Domínguez, A. (2010). *Tratamiento de datos personales y derechos fundamentales: desde Hollerith hasta Internet.* Recuperado el 17 de Abril de 2013, de Página web del programa Consolider Ingenio 2010 "El tiempo de los derechos" (HURI-AGE): http://www.tiempodelosderechos.es/docs/jun12/sq.pdf

Garzón Valdés, E. (2003). *Intimacy, privacy and publicity.* Recuperado el 16 de Febrero de 2013, de Página web de la revista "Analyse & Kritik": http://www.analyse-und-kritik.net/2003-1/AK_Garzon_2003.pdf

Geist, M. (06 de Marzo de 2012). *All your Internets Belong to US, continued: the bodog.com case.* Recuperado el 21 de Enero de 2014, de MichaelGeist.ca: http://www.michaelgeist.ca/content/view/6359/135/

Gellman, R. (3 de Octubre de 2011). *FAIR INFORMATION PRACTICES: A Basic History.* Recuperado el 13 de 10 de 2011, de bobgellman.com: http://bobgellman.com/rg-docs/rg-FIPshistory.pdf

Global Data Vault. (2012). *Data Protection - History, Evolution, Best Practices*. Recuperado el 16 de Abril de 2013, de Página web de Global Data Vault: http://www.globaldatavault.com/data-protection-whitepaper.htm

Gobiernos de Costa Rica y Canadá. (28 de Marzo de 2001). *Canada - Costa Rica joint statement on global electronic commerce.* Recuperado el 20 de Enero de 2014, de Industry canada - Government of Canada: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00382.html

Gobiernos de las Repúblicas de Costa Rica y Francia. (16 de Junio de 1998). *Acuerdo entre el Gobierno de la República de Costa Rica y el Gobierno de la República Francesa, relativo a la readmisión de personas en situación irregular.* Recuperado el 02 de Febrero de 2014, de Página web del Ministerio de Relaciones Exteriores y Culto de Costa Rica: http://www.rree.go.cr/file-ij.php?id_file=456

González Hernández, J. J. (Enero de 2007). *El derecho a la intimidad y derechos conexos. La perspectiva de su protección a nivel internacional, con enfoque especial al sistema latinoamericano y la situación actual de su reglamentación legal en México.* Recuperado el 16 de Febrero de 2013, de Vlex.com: http://vlex.com/vid/452394

González Murúa, A. R. (1994). *El derecho a la intimidad, el derecho a la autodeterminación informativa y la L.O. 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos personales.* Recuperado el 15 de marzo de 2013, de RECERCAT: Dipósit de la Recerca de Catalunya: http://www.recercat.cat/handle/2072/1371

Goyanes, M., Porangaba, & Henrique, L. (01 de Junio de 2012). *Data Protection in Brazil: overview.* Recuperado el 04 de Septiembre de 2013, de Practical Law - a Thomson Reuters legal solution: http://uk.practicallaw.com/4-520-1732#

Greenleaf, G., & Tian, G. (06 de Abril de 2013). *China expands data protection through 2013 guidelines: a "third line" for personal information protection (with a translation of the guidelines".* Recuperado el 03 de Marzo de 2014, de Social Science Research Network - Privacy Laws & Business International Report: http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2280037_code57970.pdf?abstractid=2280037&mirid=1

Greenwald, G. (09 de Agosto de 2010). *Página Web del Instituto Cato.* Recuperado el 09 de Febrero de 2011, de Cato-Unbound.org: http://www.cato-unbound.org/2010/08/09/glenn-greenwald/the-digital-surveillance-state-vast-secret-and-dangerous/

Greenwald, G., & MacAskill, E. (06 de Junio de 2013). *NSA Prism program taps in to user data of Apple, Google and others.* Recuperado el 02 de Agosto de 2013, de The Guardian: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greenwald, G., MacAskill, E., & Poitras, L. (09 de Junio de 2013). *Edward Snowden: the whistleblower behind the NSA surveillance revelations.* Recuperado el 10 de Agosto de 2013, de The Guardian: http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Guadamuz, A. (30 de Junio de 2000). *Habeas Data: The Latin American Response to Data Protection.* Recuperado el 17 de Febrero de 2012, de Warwick website: http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html

Gutierrez y González, E. (1999). *El patrimonio. El pecuniario y el moral o derechos de la personalidad.* Mexico: Porrua.

Hamlin, K. (2011). *Types of personal data.* Recuperado el 17 de Abril de 2013, de Página web del Identity Ecosystem Steering Group: https://www.idecosystem.org/sites/default/files/PersonalDataTypeMap.pdf

Hamm, S. (24 de Abril de 2008). *Cloud computing: eyes on the skies*. Recuperado el 13 de Abril de 2013, de Página web de la Bloomberg Businessweek Magazine: http://www.businessweek.com/stories/2008-04-23/cloud-computing-eyes-on-the-skies

Hampson, N. C. (01 de Mayo de 2011). *The Internet is not a lawless prairie: data protection and privacy in Italy.* Recuperado el 15 de Mayo de 2013, de Boston College International

and Comparative Law Review: http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1664&context=iclr

Hartzog, W. (2012). *Information Privacy - Chain-link Confidentiality.* Recuperado el 14 de Marzo de 2014, de Georgia Law Review: http://www.looooker.com/wp-content/uploads/2013/05/CHAIN-LINK-CONFIDENTIALITY_SSRN-id2045818.pdf

Hassemer, W., & Chirino, A. (1997). *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales.* Buenos Aires: Editores del Puerto s.r.l.

Henten, A., Samarajiva, R., & Melody, W. (2003). *Designing nexte generation telecom regulation: ICT (Information and Communication Technology) convergence or multisector utility - Report on the WDR Dialogue Theme 2002.* Ginebra: ITU.

Hernández Valle, R. (2008). Delimitación de los derechos a la intimidad y de información en la doctrina y jurisprudencia costarricense. *Estudios Constitucionales, 6*(1), 85-102.

Herrán Ortiz, A. I. (2002). *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales.* Madrid: Editorial Dykinson.

Hirsch, D. D. (2011). The law and policy of online privacy: regulation, self-regulation or co-regulation? *Seattle University Law Review, 34*(439), 439-480.

Hoffman, B. (Abril de 2008). *Why reform fails: the "politics of policies" in Costa Rican telecommunications liberalization.* Recuperado el 15 de Enero de 2014, de European Review of Latin American and Caribbean Studies: www.cedla.uva.nl/50_publications/pdf/revista/84RevistaEuropea/84Hoffmann-ISSN-0924-0608.pdf

Huxley, A. (2007). *Un Mundo Feliz.* Barcelona: Edhassa.

Instituciones de la Unión Europea. (29 de Mayo de 2009). *Cooperación en materia penal: protección de datos personales*. Recuperado el 15 de Junio de 2013, de Síntesis de la legislación de la UE: http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/jl0018_es.htm

Institute for Health Freedom. (Septiembre de 2010). *Proposed Changes to Privacy Rule Won't Ensure Privacy* . Recuperado el 20 de Agosto de 2013, de Health Freeedom Watch Newsletter: http://www.forhealthfreedom.org/Newsletter/September2010.html#Article3

Instituto de Transparencia e Información Pública de Jalisco. (2011). *Privacidad: Alcances y límites del Estado.* Recuperado el 15 de diciembre de 2012, de Página web del ITEI - Diplomado en transparencia e información pública 2011: http://www.itei.org.mx/v3/micrositios/diplomado02/gdl/adjuntos/privacidad_alcances_limites_estado.pdf

International Standards Organization. (2008). *ISO 22307:2008*. Recuperado el 13 de Octubre de 2013, de Financial services -- Privacy impact assesment: http://www.iso.org/iso/catalogue_detail?csnumber=40897

International Standards Organization. (2013). *Standards*. Recuperado el 13 de Octubre de 2013, de Página web de la International Standards Organization: http://www.iso.org/iso/home/standards.htm

International Telecommunications Union. (1994). *Constitution and convention of the International Telecommunication Union (published in Final Acts of the Addititonal Prenipotentiary Conference).* Recuperado el 05 de Enero de 2014, de ITU - Constitution and Convention: http://www.itu.int/dms_pub/itu-s/oth/02/09/s020900000d5201pdfe.pdf

International Working Group on Data Protection in Telecommunications. (04 de Marzo de 2008). *Report and Guidance on Privacy in Social Network Services - "Rome Memorandum".* Recuperado el 18 de Mayo de 2013, de Página web del Comisionado para la Protección de Datos y Libertad de Información: http://www.datenschutz-berlin.de/attachments/897/675.36.5.pdf?1347350362

Inter-Parliamentary Union. (2005). *Human Rights Handbook for Parlamentarians.* Recuperado el 09 de Febrero de 2013, de Página web de la IPU: http://www.ipu.org/pdf/publications/hr_guide_en.pdf

Intuit Inc. (2013). *A timeline of Database History*. Recuperado el 13 de Abril de 2103, de Página web de Intuit Inc.: http://quickbase.intuit.com/articles/timeline-of-database-history

Ishimaru & Associates LLP. (28 de Agosto de 2012). *Strenghtening Internet Information Protection (unnoficial English translation).* Recuperado el 05 de Octubre de 2013, de Página web de Ishimaru & Associates LLp: http://ishimarulaw.com/strengthening-network-information-protectionoctober-china-bulletin/

ISO 27000 Newsletter. (2006). *ISO 27000 Newsletter: News & Updates for ISO 27001 and ISO27002*. Recuperado el 13 de Octubre de 2013, de ISO 27000 News: http://17799-news.the-hamster.com/

ISO/IEC. (15 de Diciembre de 2011). *ISO/IEC 29100: Information Technology - Security Techniques - Privacy Framework*. Recuperado el 13 de Octubre de 2013, de Página web de IEC: http://webstore.iec.ch/preview/info_isoiec29100%7Bed1.0%7Den.pdf

IT Governance Ltd. (05 de Diciembre de 2011). *ISO29100 (ISO 29100) Privacy Framework*. Recuperado el 13 de Octubre de 2013, de Página web de IT Governance para los Estados Unidos de América: http://www.itgovernanceusa.com/shop/p-1280-iso29100-iso-29100-privacy-framework.aspx#.UlpRMRDm53s

IT Law Wiki. (2013). *HITECH Act.* Recuperado el 29 de Agosto de 2013, de Página web de la IT Law Wiki: http://itlaw.wikia.com/wiki/HITECH_Act

Jenkins, H. (2006). *Convergence culture, where old and new media collide.* New York: New York University Press.

Jiménez Vargas, M. E. (2003). *Protección de la intimidad y control de datos. Propuesta para una regulación integral en Costa Rica. Trabajo final de graduación para optar por el grado de licenciatura en Derecho.* San José: Universidad de Costa Rica.

Kartzi, M. (2008). *Making Connections: social network sites, privacy and law.* Toronto: University of Toronto.

Katz, R. H. (2 de Abril de 1997). *The International Telegraph Union.* Recuperado el 07 de Noviembre de 2013, de Página web de la Universidad de Berkeley: http://bnrg.cs.berkeley.edu/~randy/Courses/CS39C.S97/regulation/regulation.html

Kirk, S., Frazer, J., & Vincenti, J. (2007). Is Big Business Watching You? RFID Tags, Data Protection and the Retail Industry in the European Union. *The Computer and Internet Lawyer, 24*(2), 1-5.

Kirsh, E. M., Phillips, D. W., & McIntyre, D. E. (Septiembre de 1996). *Recommendations for the Evolution of Cyberlaw.* Recuperado el 12 de Enero de 2012, de Journal of Computer-Mediated Communication, University of Indiana: jcmc.indiana.edu/vol2/issue2/jcmc223.htm

Kirsh, E., Philips, D., & McIntyre, D. (1996). *Recommendations for the Evolution of Netlaw: Protecting Privacy in a Digital Age.* Recuperado el 31 de Agosto de 2013, de Journal of Computer-Mediated Communication: http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.1996.tb00056.x/full

Komukai, T. (Septiembre de 2013). *Data Protection in Japan, Regulation and Discussion.* Recuperado el 04 de Octubre de 2013, de Página web del Asia Pacific Regional Internet Governance Forum 2013: http://2013.rigf.asia/wp-content/uploads/2013/09/Privacy%20in%20Asia%20%20Building%20on%20the%20APEC%20Privacy%20Principles%20-%20Taro%20Komukai.pdf

Kosinski, M., Stillwell, D., & Graepel, T. (11 de Marzo de 2013). *Private traits and attributes are predictable from digital records of human behavior.* Recuperado el 11 de Marzo de 2013, de Proceedings of the National Academy of Sciences of the United States of America: http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html

Kozloff, N. (17 de Julio de 2013). *Snowden aftermath: why is Obama fixated on the "Switzerland of Latin America"?* Recuperado el 14 de Mayo de 2014, de Página web del Huffington Post: http://www.huffingtonpost.com/nikolas-kozloff/snowden-aftermath-why-is_b_3613962.html

Larose, C. J., & Siripurapu, J. M. (28 de Junio de 2013). *Guide to compliance with the Ammended Children's Online Privacy Protection Act (COPPA) Rule*. Recuperado el 07 de Agosto de 2013, de The national law review:

http://www.natlawreview.com/article/guide-to-compliance-amended-children-s-online-privacy-protection-act-coppa-rule

Larson, A. (2011). *The Fair Debt Collection Practices Act (FDCPA).* Recuperado el 28 de Agosto de 2013, de Página web de ExpertLaw: http://www.expertlaw.com/library/consumer/fair_debt_collection.html

Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., y otros. (Octubre de 2009). *A brief history of the Internet.* Recuperado el 02 de Febrero de 2013, de Página web de la Universidad de California, Santa Bárbara: http://www.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf

Leiva, A. M. (2012). *Data protection law in Spain and Latin América: Survey of Legal Approaches.* Recuperado el 03 de Octubre de 2013, de International News - American Bar Association: http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html

Lewis University. (2013). *A brief history of Information Security*. Recuperado el 16 de Abril de 2013, de Masters of Science in Information Security - Lewis University: http://www.lewisu.edu/academics/msinfosec/history.htm

Lind, J. (Junio de 2004). *Convergence, history of term usage and lessons from strategists.* Recuperado el 15 de Enero de 2014, de Center for information and communications research: http://userpage.fu-berlin.de/~jmueller/its/conf/berlin04/Papers/1_LIND.doc

Linskey, O., Robinson, N., & Greenberg, M. (Noviembre de 2010). *e-Discovery and legal frameworks concerning Privacy and Data Protection in European Countries.* Recuperado el 01 de Septiembre de 2013, de RAND Europe: http://www.ftitechnology.com/doc/White-Papers/whitepaper-rand-implications-part-one-2010.pdf

Lions, M. (febrero de 1969). *Los derechos humanos en la historia y la doctrina.* Recuperado el 20 de enero de 2013, de Página web del Instituto de Investigaciones Jurdicas de la UNAM: http://biblio.juridicas.unam.mx/libros/2/848/22.pdf

López Neira, A., & Ruiz Spohr, J. (2005). *ISO 27000.* Recuperado el 13 de Octubre de 2013, de Portal de ISO 27001 en español: http://www.iso27000.es/iso27000.html

López Vargas, J. A., & Torres Granados, M. d. (2010). *Problemática del delito informático: Hacia una necesaria regulación internacional. Trabajo final de graduación para optar por el grado de licenciatura en Derecho.* San José: Universidad de Costa Rica.

López-Ayllón, S. (2000). *El derecho a al información como Derecho Fundamental.* Recuperado el 10 de Marzo de 2013, de Página web de la Universidad Nacional Autónoma de México: http://biblio.juridicas.unam.mx/libros/1/7/5.pdf

Lozano, C. (2009). Teoría Dogmática de los Derechos Humanos. En U. L. Cátedra Gerardo Molina, *Derechos económicos, sociales y culturales* (págs. 35-60). Bogotá: Editorial Kimbres Ltda.

Lynch, B. (07 de Agosto de 2012). *Do not track in the Windows 8 setup experience*. Recuperado el 13 de Octubre de 2013, de Microsoft on the Issues: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/08/07/do-not-track-in-the-windows-8-set-up-experience.aspx

Maciel, M., Souza, P. d., & Affonso, C. (Septiembre de 2011). *Multi-stakeholder participation on internet governance: an analysis from a developing country, civil society perspective.* Recuperado el 04 de Septiembre de 2013, de Association for progressive communications: https://www.apc.org/fr/system/files/NoN_Multistakeholder_InternetGovernance.pdf

Madrigal Alfaro, L. (2011). *Las apuestas por internet: Régimen jurídico aplicable, Trabajo final de graduación para optar al grado de Licenciatura en Derecho.* San José: Universidad de Costa Rica.

Manolescu, D. (17 de Junio de 2010). *Data protection as a fundamental right.* Recuperado el 06 de Junio de 2013, de Effectius.com: http://effectius.com/yahoo_site_admin/assets/docs/Data_protection_as_a_fundamental_right_Dan_Manolescu_Issue5.16761659.pdf

Mari, A. (10 de Julio de 2013). *"Internet Constitution" becomes priority for Brazilian government.* Recuperado el 04 de Septiembre de 2013, de zdnet.com: http://www.zdnet.com/internet-constitution-becomes-priority-for-brazilian-government-7000017839/

Mari, A. (16 de Agosto de 2013). *Google and Facebook express concern over data protection laws in Brazil.* Recuperado el 04 de Septiembre de 2013, de zdnet.com: http://www.zdnet.com/google-and-facebook-express-concern-over-data-protection-laws-in-brazil-7000019508/

Martí de Gidi, L. d. (Enero-Junio de 2001). *El derecho a la información en México. Situación y propuesta.* Recuperado el 10 de Marzo de 2013, de Página web de la revista Letras Jurídicas, Universidad de Veracruz: http://www.letrasjuridicas.com/Volumenes/3/marti3.pdf

Martin, E. (2009). *Oxford Dictionary of Law.* Oxford: Oxford University Press.

Martínez-Herrera, M. (Septiembre de 2011). *From Habeas Data Action to Omnibus Data Protection: The Latin American Privacy (R)Evolution*. Recuperado el 3 de Septiembre de 2013, de White & Case LLP: http://www.whitecase.com/files/Publication/e5d9876a-bf18-4267-8de7-723c3121e009/Presentation/PublicationAttachment/ab31c92c-c423-4bcb-a7d7-74c822baaa22/article_From_Habeas_Data_Action_to_Omnibus_Data_Protection.pdf

Mayer, J. (07 de Abril de 2009). *"Any person... a pamphleteer" Internet Anonymity in the Age of Web 2.0.* Recuperado el 21 de Mayo de 2013, de academia.edu: www.academia.edu/attachments/30738421/download_file

Mayer, J., Narayanan, A., & Stamm, S. (07 de Marzo de 2011). *Do not track draft standard specification.* Recuperado el 16 de Mayo de 2013, de Página web de la Internet Engineering Task Force: http://datatracker.ietf.org/doc/draft-mayer-do-not-track/

Mayorga Angulo, N., & Ulloa Montoya, R. (2011). *Protección al consumidor final costarricense en caso de incumplimiento en la compraventa por internet. Trabajo final de graduación para optar por el título de Licenciatura en Derecho.* San José: Universidad de Costa Rica.

Mc Afee, Inc. (2013). *Equal Credit Opportunity Act (ECOA).* Recuperado el 28 de Agosto de 2012, de US & Global Data Protection Laws - US Federal Laws and Regulations: http://www.mcafee.com/us/regulations/north-america/us/federal/equal-credit-opportunity-act.aspx

McAfee, Inc. (2013). *Communications Assistance for Law Enforcement (CALEA)*. Recuperado el 04 de Agosto de 2013, de US & Global Data Protection Laws -US Federal Laws and Regulations: http://www.mcafee.com/us/regulations/north-america/us/federal/communications-assistance-law-enforcement-act.aspx

McAfee, Inc. (2013). *Computer Fraud and Abuse Act of 1984 (CFAA)*. Recuperado el 03 de Agosto de 2013, de US & Global Data Protection Laws - US Federal Laws and Regulations: http://www.mcafee.com/us/regulations/north-america/us/federal/computer-fraud-abuse-act.aspx

McAfee, Inc. (2013). *Computer Matching and Privacy Protection Act*. Recuperado el 04 de Agosto de 2013, de US & Global Data Protection Laws - US Federal Laws and Regulations: http://www.mcafee.com/us/regulations/north-america/us/federal/computer-matching-privacy-protection-act.aspx

McAfee, Inc. (2013). *Electronic Communications Privacy Act (ECPA).* Recuperado el 05 de Agosto de 2013, de US & Global Data Protection Laws - US Federal Laws and Regulations: http://www.mcafee.com/us/regulations/north-america/us/federal/electronic-communications-privacy-act.aspx

McAfee, Inc. (2013). *Gramm-Leach-Bliley Financial Modernization Act (GLBA).* Recuperado el 29 de Agosto de 2013, de US & Global Data Protection Laws - US Federal Laws and Regulation: http://www.mcafee.com/us/regulations/north-america/us/federal/gramm-leach-bliley-financial-modernization-act.aspx

McAfee, Inc. (2013). *Identity Theft and Assumption Deterrence Act.* Recuperado el 29 de Agosto de 2013, de US & Global Data Protection Laws - US Federal Laws and Regulations: http://www.mcafee.com/us/regulations/north-america/us/federal/identity-theft-assumption-deterrence-act.aspx

McAfee, Inc. (2013). *Right to Financial Privacy Act (RFPA).* Recuperado el 30 de Agosto de 2013, de US & Global Data Protection Laws - US Federal Laws and Regulations: http://www.mcafee.com/us/regulations/north-america/us/federal/right-financial-privacy-act.aspx

McCullagh, D., & Van Grove, J. (04 de Abril de 2013). *Apple's iMessage encryption trips up feds' surveillance*. Recuperado el 04 de Abril de 2013, de cnet.com: http://news.cnet.com/8301-13578_3-57577887-38/apples-imessage-encryption-trips-up-feds-surveillance/

McDermott Will & Emery. (3 de Enero de 2013). *Decision on Strenghtening the Protection of Online Information.* Recuperado el 02 de Marzo de 2014, de Página web de McDermott Will & Emery: http://www.mwe.com/Decision-on-Strengthening-the-Protection-of-Online-Information-01-03-2013/

Medina Riestra, A. (1999). *Teoría del Derecho Civil.* Guadalajara: Porrua.

Mendel, T. (2009). *El derecho a la información en América Latina, Comparación Jurídica.* Recuperado el 10 de mayo de 2013, de Página web de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura: http://unesdoc.unesco.org/images/0018/001832/183273s.pdf

Méndez, M., Marín, A., & Steller, L. (19 de Diciembre de 2013). Sobre protección de datos personales y estándares abiertos. (A. Quesada Rodríguez, Entrevistador) San José, Costa Rica.

Michael, J. (1994). *Privacy and Human Rights: an international and comparative study with special reference to developments in information technology.* Londres: Dartmouth.

Millán Salas, F., & Peralta Ortega, J. C. (1995). *El derecho de autodeterminación informativa como derecho de la personalidad o derecho fundamental.* Recuperado el 16 de Marzo de 2013, de Página web de la Universidad Complutense de Madrid: http://revistas.ucm.es/index.php/CESE/article/view/CESE9595110203A/10788

Miller, A. (1971). *The Assault on Privacy.* Ann Arbor: University of Michigan Press.

Miller, D. D. (2011). *Brave New World and the Threat of Technological Growth.* Recuperado el 22 de Octubre de 2013, de StudentPulse: www.studentpulse.com/articles/509/brave-new-world-and-the-threat-of-technological-growth

MINAET - Viceministerio de Telecomunicaciones. (2009). *Informe 1 - Diagnóstico PNDT.* Recuperado el 07 de Enero de 2014, de Superintendencia de Telecomunicaciones: http://telecom.go.cr/index.php/plan-nacional-de-desarrollo/telecom/publicaciones/pndt/diagnostico/download

MINAET - Viceministerio de Telecomunicaciones. (Noviembre de 2012). *Informe de Evaluación - Plan Nacional de Desarrollo de las Telecomunicaciones 2009-2014.* Recuperado el 05 de Febrero de 2014, de Ministerio de Ciencia, Tecnología y Telecomunicaciones de

Costa Rica: http://www.telecom.go.cr/index.php/plan-nacional-de-desarrollo/telecom/publicaciones/pndt/informe-de-evaluacion-pndt-2009-2014-nov-2012/download

Ministerio de Ciencia, Tecnología y Telecomunicaciones. (09 de Abril de 2013). *Decreto Ejecutivo Nº 46-H-MICITT "Las instituciones del sector público privilegiarán la adquisición de soluciones de cómputo en la nube sobre otro tipo de infraestructura".* Recuperado el 01 de Mayo de 2014, de Sistema Costarricence de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74850&nValor3=92560&param2=1&strTipM=TC&lResultado=3&strSim=simp

Ministerio de Economía, Industria y Comercio . (09 de Septiembre de 2013). *Decreto Ejecutivo Nº 37899 "Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor N° 7472".* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurdica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=75696&nValor3=94000&strTipM=TC

Ministerio de Justicia de Canadá. (16 de Marzo de 2014). *Library and Archives of Canada Act.* Recuperado el 15 de Abril de 2014, de Página web del Ministerio de Justicia de Canadá: http://laws-lois.justice.gc.ca/PDF/L-7.7.pdf

Ministerio de Justicia de Canadá. (16 de Marzo de 2014). *Personal Information Protection and Electronic Documents Act.* Recuperado el 15 de Abril de 2014, de Página web del Ministerio de Justicia de Canadá: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

Ministerio de Justicia de Canadá. (16 de Marzo de 2014). *Privacy Act.* Recuperado el 15 de Abril de 2014, de Página web del Ministerio de Justicia de Canadá: http://laws-lois.justice.gc.ca/PDF/P-21.pdf

Ministerio de Justicia de Japón. (1 de Abril de 2009). *Act on the Protection of Personal Information.* Recuperado el 04 de Octubre de 2013, de Japanese Law Translation Database System: http://www.japaneselawtranslation.go.jp/law/detail/?id=130&vm=04&re=02

Ministerio de Justicia y Paz. (04 de Abril de 2014). *Las personas físicas o jurídicas públicas o privadas propietarias o administradoras de bases de datos deberán adecuar sus procedimientos y reglas de actuación para cumplir con Ley N° 8968 Protección de la Persona frente tratamiento datos personales .* Recuperado el 22 de Julio de 2014, de Sistema Costarricense de Información Pública: http://196.40.56.11/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=77324&nValor3=96852&strTipM=TC

Ministerio del Ambiente, Energía y Telecomunicaciones. (Agosto de 2009). *Análisis de antecedentes, prácticas comerciales y tecnológicas de cinco operadores de telefonía móvil potencialmente entrantes en el mercado costarricense.* Recuperado el 01 de

Mayo de 2011, de Página web de INFOCOM: http://www.infocom.cr/downloads/docs/Info%20sector%20telecom/Analisis%20Rectoria%20cinco%20operadores%20de%20telefonia%20movil%20potenciales.pdf

Ministerio del Interior de la República Federativa del Brasil. (1 de Enero de 1988). *Constitución Política de la Republica Federativa del Brasil, 1988.* Recuperado el 03 de Septiembre de 2013, de refworld.org: http://www.refworld.org/docid/3db937cd2.html

Miniwatts Marketing Group. (16 de Julio de 2011). *Costa Rica Internet usage, broadband and telecommunications reports*. Recuperado el 15 de Mayo de 2013, de Internet World Stats: http://www.internetworldstats.com/am/cr.htm

Miralles, R. (Diciembre de 2010). Informàtica en núvol i protecció de dades / Cloud Computing and Data Protection. *Revista dels Estudis de Dret i Ciència Política de la UOC*(11).

Miyara, F. (2004). *Conversores D/A y A/D.* Recuperado el 24 de Octubre de 2013, de Página web de la Universidad Nacional del Rosario: http://www.fceia.unr.edu.ar/enica3/da-ad.pdf

Moncau, Luiz Fernando; Nicoletti Mizukami, Pedro. (25 de Marzo de 2014). *Brazilian Chamber of Deputies Approves Marco Civil Bill.* Recuperado el 25 de Marzo de 2014, de Infojustice.org: http://infojustice.org/archives/32527

Morales Godo, J. (2002). *Derecho a la Intimidad.* Recuperado el 16 de Febrero de 2013, de vlex.com: https://sibdi.ucr.ac.cr/http://vlex.com.pe/source/derecho-intimidad-4626

Morales Godo, J. (2009). *Instituciones del Derecho Civil.* Lima: Palestra Editores.

Morales Viales, R., & Ugarte Ibarra, R. (2012). *Tutela de los derechos de la personalidad virtual y protección de datos de carácter personal en las redes sociales online.* Recuperado el 15 de Noviembre de 2012, de Página Web del Instituto de Investigaciones Jurídicas de la Universidad de Costa Rica: www.iij.ucr.ac.cr/download/file/fid/627

Mosing, M. W. (Enero de 2003). *Cookies and Log Files the "transparent Internet user" or data protection on the Internet in the EU!?* Recuperado el 16 de Mayo de 2013, de it-law.at: http://www.it-law.at/uploads/tx_publications/mosing_log-files_cookies_english.pdf

Mozilla Inc. (2014). *Lightbeam.* Recuperado el 12 de Mayo de 2014, de Página web de Lightbeam: http://www.mozilla.org/es-ES/lightbeam/

Murillo de la Cueva, P. L. (Septiembre de 2007). *Perspectivas del derecho a la autodeterminación informativa.* Recuperado el 15 de Marzo de 2013, de IDP. Revista de Internet, Derecho y Política: http://www.uoc.edu/idp/5/dt/esp/lucas.pdf

National Telecommunications & Information Administration. (25 de Julio de 2013). *Privacy Multistakeholder Process: Mobile Application Transparency.* Recuperado el 31 de Agosto de 2013, de Página web de NTIA: http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency

Nikken, P. (2010). *La protección de los derechos humanos: haciendo efectiva la progresividad de los derechos económicos, sociales y culturales.* Recuperado el 03 de febrero de 2013, de Página web de la Corte Interamericana de Derechos Humanos: http://www.corteidh.or.cr/tablas/r25563.pdf

Nino, C. (2 de Octubre de 2009). *El Concepto de Derechos Humanos.* Recuperado el 3 de Febrero de 2013, de Página web de la Universidad de Congreso, Argentina: http://w3.ucongreso.edu.ar/wp-content/uploads/2009/10/2.-El-Concepto-de-DDHH-Nino.pdf

North American Leaders Summit. (01 de Enero de 2013). *Report on the Trilateral Committee on Transborder Data Flows.* Recuperado el 21 de Mayo de 2013, de Página web del Ministerio de Industria de Canadá: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Report_Trilateral_Committee_Jan_2010.pdf/$FILE/Report_Trilateral_Committee_Jan_2010.pdf

Nughter, A. (1990). *Transborder flow of personal data within the EC.* Boston: Klower.

Office of Communications. (2008). *Communication Market Report.* Londres: Office of Communications.

Office of the Press Secretary - The White House. (23 de Febrero de 2012). *Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights.* Recuperado el 23 de Febrero de 2012, de www.whitehouse.gov: www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

Office of the Press Secretary - The White House. (23 de Febrero de 2012). *We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online.* Recuperado el 31 de Agosto de 2013, de whitehouse.gov: http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights

O'Hara, K. (26 de Abril de 2010). *Intimacy 2.0: Privacy rights and privacy responsabilities on the World Wide Web.* Recuperado el 16 de Febrero de 2013, de Página web de "The Web Science Trust": http://journal.webscience.org/294/

Ohm, P. (2009). Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, 1703-1776.

Onn, Y. (2005). *Privacy in the Digital Environment.* Haifa: Haifa Center of Law & Technology.

Open Rights Group. (11 de Enero de 2013). *Data Retention Directive*. Recuperado el 15 de Junio de 2013, de Data Retention Directive - Open Rights Group: http://wiki.openrightsgroup.org/wiki/Data_Retention_Directive

Open Society Justice Initiative. (Octubre de 2011). *Principios sobre seguridad nacional y el derecho a la información.* Recuperado el 10 de Marzo de 2013, de Página web de la

Open Society Justice Initiative: www.right2info.org/resources/publications/national-security-principles-in-spanish-10.2011

Organización de Estados Americanos. (03 de Abril de 2012). *Comparative Study: data Protection in the Americas.* Recuperado el 15 de Abril de 2014, de Página web de la OEA: http://www.oas.org/es/sla/ddi/docs/CP-CAJP-3063-12_en.pdf

Organización de las Naciones Unidas. (10 de Diciembre de 1948). *Declaración Universal de los Derechos Humanos.* Recuperado el 03 de Marzo de 2013, de Página web de la Organización de las Naciones Unidas: http://www.un.org/es/documents/udhr/

Organización de las Naciones Unidas. (16 de Diciembre de 1966). *Pacto Internacional de Derechos Civiles y Políticos.* Recuperado el 04 de Marzo de 2013, de Página web de la oficina del alto comisionado de las Naciones Unidas para los Derechos Humanos: www2.ohchr.org/spanish/law/ccpr.htm

Organización de las Naciones Unidas. (16 de Diciembre de 1966). *Pacto Internacional de Derechos Económicos, Sociales y Culturales.* Recuperado el 04 de Marzo de 2013, de Página web de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos: http://www2.ohchr.org/spanish/law/cescr.htm

Organización de las Naciones Unidas. (07 de Octubre de 1998). *Estatuto de Roma de la Corte Penal Internacional.* Recuperado el 25 de Febrero de 2014, de Página web de las Naciones Unidas: http://www.un.org/spanish/law/icc/statute/spanish/rome_statute%28s%29.pdf

Organización de las Naciones Unidas. (25 de mayo de 2000). *Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.* Recuperado el 02 de Marzo de 2014, de Oficina del alto comisionado de las Naciones Unidas para los Derechos Humanos: http://www2.ohchr.org/spanish/law/crc-sale.htm

Organización de las Naciones Unidas. (08 de Noviembre de 2005). *Tunis Agenda for the Information Society.* Recuperado el 15 de Mayo de 2013, de World Summit on the Information Society: http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf

Organización de las Naciones Unidas. (20 de Junio de 2006). *Convención Internacional para la protección de todas las Personas contra las Desapariciones Forzadas.* Recuperado el 06 de Marzo de 2014, de Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos: http://www2.ohchr.org/spanish/law/disappearance-convention.htm

Organización de las Naciones Unidas. (2012). *Derechos Humanos*. Recuperado el 06 de Febrero de 2013, de Página Web de las Naciones Unidas: http://www.un.org/es/globalissues/humanrights/

Organización de los Estados Americanos. (22 de noviembre de 1969). *Convención Americana sobre Derechos Humanos.* Recuperado el 04 de Marzo de 2013, de Página web de la

Organización de los Estados Americanos: http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

Organización de los Estados Americanos. (25 de Febrero de 1981). *Convención Interamericana sobre Extradición.* Recuperado el 03 de Marzo de 2014, de Página web de la OEA: http://www.oas.org/juridico/spanish/tratados/b-47.html

Organización de los Estados Americanos. (Abril de 2008). *Guía de Mecanismos para la promoción de la transparencia y la integridad en las Américas*. Recuperado el 11 de Abril de 2013, de Página web de la Organización de los Estados Americanos: http://www.oas.org/es/sap/dgpe/guia_egov.asp

Organización de los Estados Americanos. (31 de Octubre de 2011). *Cuestionario de Legislación y Prácticas sobre Privacidad y Protección de Datos [AG/RES.2661 (XLI-O/11)].* Recuperado el 21 de Enero de 2014, de Página web de la OEA: http://www.oas.org/dil/esp/proteccion_de_datos_cuestionario_Costa_Rica.pdf

Organización para la Cooperación y el Desarrollo Económico. (23 de Septiembre de 1980). *Directrices relativas a la protección de la intimidad y de la circulazión transfronteriza de datos personales.* Recuperado el 06 de Mayo de 2013, de Página web del Instituto Federal de Acceso a la Información y Protección de Datos de México: http://inicio.ifai.org.mx/DocumentosdeInteres/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad.pdf

Organización para la Cooperación y el Desarrollo Económico. (Septiembre de 1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Recuperado el 07 de Octubre de 2013, de Página web de la OECD: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Organización para la Cooperación y el Desarrollo Económico. (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Recuperado el 16 de Abril de 2013, de Página web de la Organización para la Cooperación y el Desarrollo Económico: http://www.oecd.org/internet/ieconomy/34912912.pdf

Organización para la Cooperación y el Desarrollo Económico. (11 de Julio de 2013). *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.* Recuperado el 07 de Octubre de 2013, de Página web de la OECD: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Orric, Herrington & Suitcliffe LLP. (Agosto de 2002). *Securities Law Update.* Recuperado el 30 de Agosto de 2013, de Página web del Instituto de Gobierno Corporativo Costa Rica: www.igc-costarica.org/inc/download.php?file=19

Pappas, L. A. (07 de Enero de 2013). *China Enacts Online Privacy Framework To Protect Data, but Not User Anonymity.* Recuperado el 05 de Octubre de 2013, de Bloomberg BNA: http://www.bna.com/china-enacts-online-n17179871719/

Parenti, C. (2003). *The soft cage: Surveillance in America from slave passes to the war on terror.* New York: Free Press.

Parlamento Europeo. (17 de Junio de 2013). *2012/0011(COD) - 25/01/2012 Legislative Proposal (Summary)*. Recuperado el 17 de Junio de 2013, de Página web del parlamento europeo: http://www.europarl.europa.eu/oeil/popups/summary.do?id=1188884&t=d&l=en

Parlamento Europeo y Consejo de la Unión Europea. (23 de Noviembre de 1995). *Directiva 95/46 EC.* Recuperado el 01 de Junio de 2013, de Diario Oficial de las Comunidades Europeas - Página web oficial de la Unión Europea: eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:pdf

Parlamento Europeo y Consejo de la Unión Europea. (18 de Diciembre de 2000). *Reglamento (CE) Nº 45/2001.* Recuperado el 15 de Junio de 2013, de Diario oficial de las Comunidades Europeas - Página web oficial de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:ES:PDF

Parlamento Europeo y Consejo de la Unión Europea. (12 de Julio de 2002). *Directiva 2002/58/CE.* Recuperado el 15 de Junio de 2013, de Diario Oficial de las Comunidades Europeas - Página web oficial de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:es:pdf

Parlamento Europeo y Consejo de la Unión Europea. (13 de Abril de 2006). *Directiva 2006/24/CE.* Recuperado el 15 de Junio de 2013, de Diario Oficial de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:es:pdf

Parlamento Europeo y Consejo de la Unión Europea. (25 de Noviembre de 2009). *Directiva 2009/136/CE.* Recuperado el 04 de Junio de 2013, de Diario Oficial de la Unión Europea - Página web oficial de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:es:PDF

Parlamento Europeo, Consejo de la Unión Europea y Comisión Europea. (18 de Diciembre de 2000). *Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01) (art 8).* Recuperado el 06 de Junio de 2013, de Página web del Parlamento europeo: http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Parsons, C. (6 de Febrero de 2013). *(Draft) Chapter One: Deep Packet Inspection and it's predecessors, v.3.5.* Recuperado el 10 de Abril de 2013, de Technology, Thoughts and Trinkets (blog): http://www.christopher-parsons.com/Main/wp-content/uploads/2013/02/DPI-and-Its-Predecessors-3.5.pdf.

Peña Ortiz, P., & Achío Gutiérrez, C. (2011). *El Derecho al Olvido, Trabajo final de graduación para optar por el grado de Licenciatura en Derecho.* San José: Universidad de Costa Rica.

Pérez Fuentes, G. M. (2004). *Evolución doctrinal, legislativa y jurisprudencial de los derechos de la personalidad y el daño moral en España.* Recuperado el 05 de enero de 2013, de Dialnet - Revista de Derecho Privado (UNAM): http://dialnet.unirioja.es/servlet/articulo?codigo=951053&orden=22155&info=link

Pérez González, D. E. (2001). *Problemática de la colisión entre los derechos de la personalidad y la libertad de expresión e información - Solución doctrinal y jurisprudencial.* Recuperado el 05 de enero de 2013, de Dialnet - Anuario de la Facultad de Derecho, Universidad de Extremadura: http://dialnet.unirioja.es/descarga/articulo/831686.pdf

Pérez Luño, A. (1987). *Nuevas tecnologías, Sociedad y Derecho.* Madrid: Fundesco.

Pérez Luño, A. (1992). Vittorio Frosini y los nuevos derechos de la sociedad tecnológica. *Informatica e Diritto*, 104.

Pérez Luño, A. (2000). *La tutela de la libertad informatica en la sociedad globalizada.* Recuperado el 05 de Abril de 2013, de Página web de ISEGORIA, revista de filosofía moral y política del Instituto de Filosofía del Consejo Superior de Investigaciones Científicas de España: http://isegoria.revistas.csic.es/index.php/isegoria/article/viewArticle/521

Pérez Luño, A. E., Soriano Díaz, R. L., & Gómez Torres, C. J. (2004). *Diccionario jurídico: Filosofía y teoría del derecho e informática jurídica.* Granada: Comares.

Pérez Martínez, J. (2005). *Evolución y Tendencias del Sector de las Telecomunicaciones.* Recuperado el 02 de Mayo de 2011, de Internet de Nueva Generación - Cátedra Telefónica en la Universidad Politécnica de Madrid: http://internetng.dit.upm.es/ponencias-jing/2005/jorge.pdf

Pérez, J., & Ramos, S. (31 de Enero de 2007). *La participación de la sociedad actual en la gobernanza de Internet.* Recuperado el 11 de Abril de 2013, de Página web del Internet Governance Forum España: http://www.igfspain.com/doc/archivos/Temas-para-el-Debate-Gobernanza.pdf

Personal Data Ecosystem Consortium. (7 de Abril de 2011). *Personal Data 2.0 - Igniting the Personal Data Ecosystem.* Recuperado el 17 de Abril de 2013, de Página web del Personal Data Ecosystem Consortium: http://pde.cc/wp-content/uploads/2011/11/PersonalData2-PaloAlto.pdf

Pfeffer Urquiaga, E. (2000). *Los derechos a la intimidad o privacidad, a la honra y a la propia imagen. Su protección frente a la libertad de opinión e información.* Recuperado el 16 de Febrero de 2013, de Página web de la Universidad de Talca: http://redalyc.uaemex.mx/pdf/197/19760123.pdf

Pinedo Aubián, F. (s.f.). *El principio de la autonomía de la voluntad y la conciliación extrajudicial.* Recuperado el 26 de Febrero de 2013, de Página web de la Escuela Nacional de la Judicatura, República Dominicana: http://enj.org/portal/biblioteca/penal/rac/32.pdf

Pisent Masons LLP. (Febrero de 2013). *China Protection Update - China Publishes New Privacy Standard.* Recuperado el 05 de Octubre de 2013, de Página web de Pisent Masons: http://www.pinsentmasons.com/PDF/DataProtectionUpdateFeb13.pdf

Poder Ejecutivo de la República de Costa Rica. (22 de Septiembre de 2008). *Decreto Ejecutivo Nº 34765-MINAET "Reglamento a la Ley General de Telecomunicaciones".* Recuperado el 22 de Febrero de 2014, de SUTEL - Reglamentos: http://www.sutel.go.cr/Medios/Descargar/5384DA3073EAC4C626667CDECBE3E7F0E52C63E5

Poder Ejecutivo de la República de Costa Rica. (01 de Julio de 2008). *Decreto Ejecutivo Nº 34986-MP-PLAN "Reforma reglamento orgánico del Poder Ejecutivo".* Recuperado el 03 de Febrero de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=64800&nValor3=75358&strTipM=TC

Poder Ejecutivo de la República de Costa Rica. (24 de Febrero de 2009). *Decreto Ejecutivo Nº 35148-MINAET "Reglamento al título II de la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones".* Recuperado el 02 de Marzo de 2014, de Sistema Costarricense de Información Jurídica en Línea: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=65228&nValor3=80768&strTipM=TC

Poder Ejecutivo de la República de Costa Rica. (16 de Abril de 2009). *Decreto Ejecutivo Nº 35205-MINAET "Reglamento sobre medidas de protección de la privacidad de las comunicaciones".* Recuperado el 15 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=65468&nValor3=76511&strTipM=TC

Poder Ejecutivo de la República de Costa Rica. (13 de Mayo de 2009). *Plan nacional de desarrollo de las telecomunicaciones 2009 - 2014.* Recuperado el 22 de Enero de 2014, de sutel.go.cr: http://sutel.go.cr/Medios/Descargar/73535DC44477B98C0E808A47CBCDF943A4EE77C5

Poder Ejecutivo de la República de Costa Rica. (06 de Septiembre de 2011). *Decreto Ejecutivo Nº 36774-MINAET - Reglamento a la Ley General de Telecomunicaciones.* Recuperado el 11 de Enero de 2014, de Página web de la SUTEL: http://www.sutel.go.cr/Medios/Descargar/5384DA3073EAC4C626667CDECBE3E7F0E52C63E5

Poder Ejecutivo de la República de Costa Rica. (28 de Septiembre de 2011). *Decreto Ejecutivo Nº 36831-G "Reglamento de Personas Refugiadas".* Recuperado el 21 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=71376&nValor3=86629&strTipM=TC

Poder Ejecutivo de la República de Costa Rica. (05 de Marzo de 2013). *Decreto Ejecutivo Nº 37554 "Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales".* Recuperado el 16 de Marzo de 2014, de Sistema Costarricense de Información Jurídica en Línea.: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74352&nValor3=91778&strTipM=TC

Poder Ejecutivo de la República de Costa Rica. (09 de Abril de 2013). *Directriz Nº 46-H-MICITT*. Recuperado el 22 de Mayo de 2013, de Página web del diario oficial La Gaceta: http://www.gaceta.go.cr/pub/2013/05/16/COMP_16_05_2013.html#_Toc356307871

Poder Ejecutivo de la República Federativa del Brasil. (24 de Agosto de 2011). *Propuesta final del Marco Civil da Internet.* Recuperado el 04 de Septiembre de 2013, de Página web de la cámara de diputados del Brasil: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255

Poder Judicial de la República de Costa Rica. (07 de Diciembre de 2010). *Directriz para reducir la Revictimización de Niños, Niñas y Adolescentes en Condición de Discapacidad en Procesos Judiciales.* Recuperado el 16 de Marzo de 2014, de Página web del Poder Judicial: http://www.poder-judicial.go.cr/ninnos/images/libros/022.pdf

Poder Judicial de la República de Costa Rica. (31 de Mayo de 2011). *Política Judicial dirigida al Mejoramiento del Acceso a la Justicia de las Niñas, Niños, y Adolescentes en Costa Rica.* . Recuperado el 16 de Marzo de 2014, de Página web de la UNICEF: http://www.unicef.org/costarica/docs/cr_pub_Politica_Acceso_Justicia_NNA_Costa_Rica.pdf

Polakiewicz, J. (2011). Convention 108 as a global privacy standard? *International Data Protection Conference Proceedings*, (págs. 1-10). Budapest.

Poulett, Y., & Dinant, J.-M. (2007). Hacia nuevos principios de protección de datos en un nuevo entorno TIC. *Revista de Internet, Derecho y Política*(5), 33-46.

Poullet, Y. (2009). *Data protection legislation: what is at stake for our society and democracy.* Namur, Bélgica: Elsevier Ltd.

Poullet, Y., Gutwirth, S., & De Hert, P. (2010). *Data Protection in a Profiled World.* Bruselas, Bélgica: Springer Science+Business Media .

Práctica Fiscal. (Junio de 2009). Protección de datos personales, su regulación en el sector público y sus avances en el sector privado. *Práctica Fiscal, Disponible en*

*http://doctrina.vlex.com.mx/vid/personales-regulacion-avances-privado-67078790*(544), B1-B6.

Prado, E., & Franquet, R. (1998). Convergencia digital en el paraíso tecnológico: Claroscuros de una revolución. *Revista Zer Aldizkaria*(4).

Presidente de la República del Perú. (22 de Marzo de 2013). *Decreto Supremo Nº 003-2013-JUS Reglamento de la Ley de Protección de Datos Personales.* Recuperado el 06 de Septiembre de 2013, de EL Peruano: http://www.redipd.org/legislacion/common/legislacion/peru/ReglamentoLeyProtecciondeDatos22032013.pdf

Prieto Gutiérrez, J. J., & Moreno Cámara, A. (2006). *La protección de datos: la privacidad en la biblioteca de la Universidad Complutense de Madrid.* Recuperado el 13 de Abril de 2013, de Boletín de la ANABAD - e-prints in library & information science: http://eprints.rclis.org/11680/1/LA_PROTECCIÓN_DE_DATOS..pdf

Privacilla.org. (2003 de Julio de 2001). *The Computer Matching and Privacy Protection Act*. Recuperado el 04 de Agosto de 2013, de Privacy and Government: http://www.privacilla.org/government/cmppa.html

Privacy International. (12 de Diciembre de 2006). *Report: Colombia.* Recuperado el 26 de Septiembre de 2013, de Página web de Privacy International: https://www.privacyinternational.org/reports/colombia

Privacy International. (01 de Enero de 2011). *Report: Spain.* Recuperado el 03 de Octubre de 2013, de Página web de Privacy International: https://www.privacyinternational.org/reports/spain

Privacy International. (22 de Octubre de 2012). *Report: China.* Recuperado el 2013 de Octubre de 2013, de Página web de Privacy International: https://www.privacyinternational.org/reports/china

Privacy International. (2012). *Report: Paraguay - Chapter: 1. Legal Framework.* Recuperado el 03 de Septiembre de 2013, de Página web de Privacy International: https://www.privacyinternational.org/reports/paraguay/i-legal-framework

Privacy International. (Marzo de 2013). *The right to privacy in Mexico - Stakeholder Report.* Recuperado el 19 de Septiembre de 2013, de Página web de Privacy International: https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/mexico_stakeholder_report_-_privacy_international.pdf

Privacy Rights Clearinghouse. (2014). *Fact Sheet 6a: Facts on FACTA, the Fair and Accurate Credit Transactions Act .* Recuperado el 28 de Agosto de 2013, de Página web de Privacy Rights Clearinghouse: https://www.privacyrights.org/fs/fs6a-facta.htm

Programa de la Sociedad de la Información y el Conocimiento. (2006). *Informe final del proyecto diagnóstico sobre el gobierno digital en Costa Rica, Universidad de Costa Rica,*

*Centro de Investigación y Capacitación en Administración Pública; Capítulo 5: Visiones para el desarrollo de las telecomunicaciones en Costa Rica.* Recuperado el 05 de Mayo de 2011, de Página web del PROSIC: http://www.gobiernofacil.go.cr/e-gob/gobiernodigital/informes/cap5.pdf

Programa Sociedad de la Información y el Conocimiento. (Octubre de 2010). *Ciberseguridad en Costa Rica*. Recuperado el 25 de Mayo de 2013, de Página web de la Universidad de Costa Rica: http://www.kerwa.ucr.ac.cr/bitstream/handle/10669/500/libro%20completo%20Cyber.pdf?sequence=1

Przemyslaw, D., & Slawomir, K. (2009). *Fundamentals of Communications Systems.* Recuperado el 23 de Octubre de 2013, de Telecommiunications Systems and Technologies - Vol I: http://www.eolss.net/sample-chapters/c05/E6-108-01-00.pdf

Puccinelli, O. R. (Enero de 2004). Tipos y subtipos de hábeas data en América latina. (E. Astrea, Ed.) *Artículos de Doctrina*(4).

Puente de la Mora, X. (Febrero de 2007). *Privacidad de la información personal y su protección legal en Estados Unidos.* Recuperado el 16 de Febrero de 2013, de vlex.com: http://vlex.com.pe/vid/privacidad-informacion-personal-unidos-38250761

Puente de la Mora, X. (25 de Octubre de 2010). *Protección de datos personales en posesión de los particulares en México: avances y desafíos.* Recuperado el 16 de Abril de 2013, de Página web de la Biblioteca Jur´ídica Virtual del Insittuto de Investigaciones Jurídicas de la UNAM: http://biblio.juridicas.unam.mx/libros/6/2941/26.pdf

Quesada Arroyo, L. (27 de Noviembre de 2012). *Protección de derechos caninos frente a la convergencia de las telecomunicaciones.* Naranjo, Alajuela: Editorial Pochi.

Quesada Mora, J. G. (2004). *Temas sobre Derechos fundamentales y Constitucionales.* San José: IJSA.

Quiroz Ruiz, S. L. (Julio de 2004). *En torno al aprendizaje del Derecho Informático.* Recuperado el 12 de Abril de 2013, de Revista Letras Jurídicas del Centro de Estudios sobre Derecho, Globalización y Seguridad de la Universidad Veracruzana: http://www.letrasjuridicas.com/Volumenes/10/quiroz10.pdf

Rajendra, S., & Siddhartha, R. (2010). *Convergence in Information and Communication Technology Strategic and Regulatory Considerations .* Washington DC: The International Bank for Reconstruction and Development / The World Bank.

Ramesh, R. (03 de Marzo de 2014). *NHS England patient data "uploaded to Google servers", Tory MP says.* Recuperado el 05 de Mayo de 2014, de The Guardian: http://www.theguardian.com/society/2014/mar/03/nhs-england-patient-data-google-servers

Ramírez Salinas, L. A. (2003). *El habeas data.* Recuperado el 04 de Septiembre de 2013, de Página web de RMG Abogados: http://www.rmg.com.py/publicaciones/DerechoConstitucionalyPolitico/Liza_Habeas_Data.pdf

Real Academia Española. (2001). *Dato*. Recuperado el 05 de Mayo de 2013, de Diccionario de la lengua española - Vigésima segunda edición: http://lema.rae.es/drae/?val=dato

Red Iberoamericana de Protección de Datos. (21 de Mayo de 2002). *Declaración de San Lorenzo del Escorial - España.* Recuperado el 29 de Abril de 2014, de Página web de la red: http://www.redipd.org/documentacion/common/declaracion_2002_I_encuentro.pdf

Red Iberoamericana de Protección de Datos. (6 de Junio de 2003). *Declaración de La Antigua - Guatemala.* Recuperado el 29 de Abril de 2014, de Página web de la red: http://www.redipd.org/documentacion/common/declaracion_2003_II_encuentro_es.pdf

Red Iberoamericana de Protección de Datos. (28 de Mayo de 2004). *Declaración de Cartagena de Indias - Colombia.* Recuperado el 29 de Abril de 2014, de Página web de la red: http://www.redipd.org/documentacion/common/declaracion_2004_III_encuentro_es.pdf

Red Iberoamericana de Protección de Datos. (4 de Noviembre de 2005). *Declaración de Ciudad de México - México.* Recuperado el 29 de Abril de 2014, de Página web de la red: www.redipd.org/documentacion/common/declaracion_2005_IV_encuentro_pt.pdf

Red Iberoamericana de Protección de Datos. (9 de Noviembre de 2007). *Declaración de Lisboa.* Recuperado el 29 de Abril de 2014, de Página web de la red: http://www.redipd.org/documentacion/common/declaracion_2007_V_encuentro_es.pdf

Red Iberoamericana de Protección de Datos. (Noviembre de 2007). *Directrices de Armonización de Protección de Datos en la Comunidad Iberoamericana.* Recuperado el 29 de Abril de 2014, de Página web del IFAI: http://inicio.ifai.org.mx/Estudios/Directrices_de_armonizacion.pdf

Red Iberoamericana de Protección de Datos. (3 de Noviembre de 2009). *Declaración Conjunta de Madrid - España.* Recuperado el 29 de Abril de 2014, de Página web de la red: http://www.redipd.org/documentacion/common/declaracion_2009_VII_encuentro_es.pdf

Red Iberoamericana de Protección de Datos. (29 de Septiembre de 2010). *Declaración de México.* Recuperado el 29 de Abril de 2014, de Página web de la Red: http://www.redipd.org/documentacion/common/declaracion_2010_VIII_encuentro_es.pdf

Red Iberoamericana de Protección de Datos. (2011). *Declaración de la Ciudad de México.* Recuperado el 29 de Abril de 2014, de Página web de la red: http://www.redipd.org/documentacion/common/declaracion_2011_IX_encuentro_es.pdf

Red Iberoamericana de Protección de Datos. (22 de Octubre de 2012). *Declaración de Punta del Este - Uruguay.* Recuperado el 29 de Abril de 2014, de Página web de la red: http://www.redipd.org/documentacion/common/declaracion_2012_X_encuentro_es.pdf

Red Iberoamericana de Protección de Datos. (17 de Octubre de 2013). *Declaración de Cartagena de Indias - Colombia.* Recuperado el 29 de Abril de 2014, de Página web de la red: http://www.redipd.org/documentacion/common/declaracion_2013_XI_encuentro_es.pdf

Red Iberoamericanda de Protección de Datos. (2008). *Declaración de Cartagena de Indias - Colombia.* Recuperado el 29 de Abril de 2014, de Página web de la red: http://www.redipd.org/documentacion/common/declaracion_2008_VI_encuentro_es.pdf

Reitman, R. (02 de Abril de 2013). *New California "Right to Know" Act Would Let Consumers Find Out Who Has Their Personal Data -- And Get a Copy of It*. Recuperado el 02 de Abril de 2013, de Página web de la Electronic Frontier Foundation: https://www.eff.org/deeplinks/2013/04/new-california-right-know-act-would-let-consumers-find-out-who-has-their-personal

Remolina-Angarita, N. (2010). *¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?* Recuperado el 26 de Septiembre de 2013, de International Law, revista Colombiana de Derecho Internacional: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Tiene-Colombia-nivel-adecuado....Nelson-Remolina1.pdf

Rená, P. (12 de Mayo de 2014). *Marco Civil da Internet (Lei nº 12.965) » unofficial english translation.* Recuperado el 20 de Mayo de 2014, de Cultura Digital e Democracia: http://thecdd.wordpress.com/2014/05/12/marco-civil-da-internet-lei-no-12-965-unofficial-english-translation/

Representantes de los países iberoamericanos. (06 de Junio de 2003). *Declaración de la Antigua (Guatemala) con motivo del II Encuentro Iberoamericano de Protección de Datos Personales.* Recuperado el 04 de Marzo de 2014, de Página web de la Comisión Nacional de Protección de Datos de Portugal: http://www.cnpd.pt/bin/actividade/Outros/Declaracion_de_La_Antigua.HTM

Reunión Global de Multiples Interesados Sobre el Futuro de la Gobernanza de Internet "NETmundial". (24 de Abril de 2014). *NETmundial Multistakeholder Statement.* Recuperado el 14 de Mayo de 2014, de Página web de NETmundial:

http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

Rhodes, N. (2013). *ChoicePoint Inc.* Recuperado el 23 de Mayo de 2013, de answers.com: http://www.answers.com/topic/choicepoint-inc

Riascos Gómez, L. O. (16 de Abril de 1999). *El derecho a la intimidad, la visión iusinformática y el delito de los datos personales.* Recuperado el 28 de Febrero de 2013, de Tesis Doctorales en Red - Universidad de Lleida: http://www.tdx.cat/handle/10803/8137

Riascos Gomez, L. O. (2009). *La visión constitucional del habeas data.* Recuperado el 04 de Septiembre de 2013, de Revista Informática Jurídica: http://www.informatica-juridica.com/trabajos/La_vision_constitucional_del_habeas_data.asp

Riascos Gómez, L. O. (15 de Enero de 2013). *Los delitos informáticos relativos a la intimidad, los datos personales y el habeas data en el derecho colombiano.* Recuperado el 2013 de Febrero de 27, de www.informática-jurídica.com: http://www.informatica-juridica.com/trabajos/DELITOS_INFORMATICOS_Intimidad_Habeas_Data_Informatica_Juridica_Jose_Cuervo.pdf

Rincón Cárdenas, E. (2006). *Contratación Electrónica.* Bogotá: Centro editorial Universidad del Rosario.

Riofrio, M. (08 de Abril de 2013). *The 5 biggest online privacy threats of 2013*. Recuperado el 10 de Abril de 2013, de www.pcworld.com: http://www.pcworld.com/article/2031908/the-5-biggest-online-privacy-threats-of-2013.html

Rodotà, S. (05 de Mayo de 2005). *Democracia y protección de datos.* Recuperado el 23 de Mayo de 2014, de Página web de la Agencia Española de Protección de Datos: http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/DemocraciaMadrid_mayo_05.pdf

Rodotà, S. (2006). *La conservación de los datos de tráfico en las comunicaciones electrónicas.* Recuperado el 06 de Abril de 2013, de Página web de la Revista de internet, derecho y política de la Universitat Oberta de Catalunya: http://www.uoc.edu/idp/3/dt/esp/rodota.pdf

Rodríguez Illera, R. (Octubre de 2000). Las telecomunicaciones en la era de Internet. *Revista del Derecho de las telecomunicaciones e Infraestructuras en Red*(10), 23-32.

Rodríguez Pérez, M. A. (2003). *Tridimensionalismo jurídico y protección de datos personales frente a su tratamiento automatizado.* Recuperado el 06 de Abril de 2013, de SABERES, Revista de estudios jurídicos, económicos y sociales de la Universidad Alfonso X el Sabio: http://www.uax.es/publicacion/tridimensionalismo-juridico-y-proteccion-de-datos-personales-frente-a-su.pdf

Rojas Mora, G. E. (2007). *Secreto en las comunicaciones electrónicas: medios para lograr prueba válida en un proceso penal. Trabajo final de graduación para optar por el grado de licenciatura en Derecho.* San José: Universidad de Costa Rica.

Rojas Vega, M. A., & Vargas Delgado, D. (2009). *El derecho a la intimidad frente al acceso a la información y ejercicio de la libre expresión de los medios de comunicación colectiva. Trabajo final de graduación para optar por el grado de licenciatura en Derecho.* San Ramón: Universidad de Costa Rica.

Rovira Sueiro, M. E. (1997). *La responsabilidad civil derivada de los daños ocasionados al derecho al honor, a la intimidad personal y familiar y a la propia imágen.* Recuperado el 05 de enero de 2013, de Tesis doctorals en Xarxa - Universidad de la Coruña: http://hdl.handle.net/2183/1050

Rubio Navarro, A. M. (2004). *Aspectos Prácticos de la Protección de Datos de las Personas Físicas.* Madrid: J.M. Bosh Editor.

Rudgard, S. (2012). *Origins and historical context of data protection law.* Recuperado el 16 de Abril de 2013, de Página web de la International Association of Privacy Professionals: https://www.privacyassociation.org/media/pdf/publications/European_Privacy_Chapter_One.pdf

Rueda Ortiz, R. (Junio de 2009). Convergencia tecnológica: síntesis o multiplicidad política y cultural. *Signo y Pensamiento*(54), 114-130.

Ruiz Miguel, C. (1997). *La configuración constitucional del derecho a la intimidad.* Recuperado el 05 de enero de 2013, de Tesis Doctorals en Xarxa - Universidad Complutense de Madrid: http://eprints.ucm.es/2164/1/S0002101.pdf

Rule, J. B. (1973). *Private Lives and Public Surveillance.* Londres: Allen Lane.

Sagüés, N. P. (1998). *El habeas Data: su desarrollo constitucional.* Recuperado el 04 de Septiembre de 2013, de V CONGRESO IBEROAMERICANO DE DERECHO CONSTITUCIONAL: http://biblio.juridicas.unam.mx/libros/1/113/39.pdf

Sala Constitucional de la Corte Suprema de Justicia. (05 de Diciembre de 1991). *Resolución Nº 2609-91.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=87476&strTipM=T&strDirSel=directo

Sala Constitucional de la Corte Suprema de Justicia. (01 de Marzo de 1991). *Sentencia Nº 479-91.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&param2=1&nValor1=1&nValor2=86314&strTipM=T&lResultado=2

Sala Constitucional de la Corte Suprema de Justicia. (27 de Marzo de 1991). *Voto Nº 678-91.* Recuperado el 25 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&param2=1&nValor1=1&nValor2=82944&strTipM=T&lResultado=2

Sala Constitucional de la Corte Suprema de Justicia. (08 de Junio de 1994). *Resolución Nº 2680-94.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=122864&strTipM=T&strDirSel=directo

Sala Constitucional de la Corte Suprema de Justicia. (05 de Mayo de 1995). *Voto Nº 2256-95.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=100905&strTipM=T&strDirSel=directo

Sala Constitucional de la Corte Suprema de Justicia. (16 de Junio de 1997). *Voto Nº 4154-97.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica en Línea: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=110870&strTipM=T&strDirSel=directo

Sala Constitucional de la Corte Suprema de Justicia. (27 de Febrero de 1998). *Sentencia Nº 1345.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=114277&strTipM=T&lResultado=1&pgn=&pgrt=&param2=1&nTermino=&nTesauro=&tem1=&tem4=&strLib=&spe=&strTem=&strDirTe=

Sala Constitucional de la Corte Suprema de Justicia. (27 de Abril de 1998). *Sentencia Nº 2805-98.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=114951&strTipM=T&strDirSel=directo

Sala Constitucional de la Corte Suprema de Justicia. (18 de Noviembre de 1998). *Sentencia Nº 8210-98.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&param2=1&nValor1=1&nValor2=82675&strTipM=T&lResultado=1

Sala Constitucional de la Corte Suprema de Justicia. (27 de Julio de 1999). *Resolución Nº 5802-99.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=184483&strTipM=T&strDirSel=directo

Sala Constitucional de la Corte Suprema de Justicia. (13 de Septiembre de 2002). *Sentencia Nº 8996-02.* Recuperado el 20 de Febrero de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Detalle_Sentencia&nValor1=1&nValor2=224233&nValor3=29058&tem1=&strTipM=E1&lResultado=0&pgn=&pgrt=&nTermino=&nTesauro=&tem4=Sala%20Constitucional&strLib=&spe=&strTem=&strDirTe=

Sala Constitucional de la Corte Suprema de Justicia. (04 de Octubre de 2002). *Sentencia Nº 9640-02.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=226138&strTipM=T&strDirSel=directo

Sala Constitucional de la Corte Suprema de Justicia. (25 de Enero de 2002). *Voto Nº 754-02.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica en Línea: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&param2=1&nValor1=1&nValor2=199747&strTipM=T&lResultado=1

Sala Constitucional de la Corte Suprema de Justicia. (29 de Octubre de 2004). *Sentencia Nº 12239.* Recuperado el 28 de Abril de 2014, de Sistema Costarricense de Información Jurídica: http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=293758&strTipM=T&lResultado=0&pgn=&pgrt=&param2=1&nTermino=&nTesauro=&tem1=sociedad%20recurrida%20ofrece%20servicios%20recopilaci%C3%B3n%20dato

Sala Constitucional de la Corte Suprema de Justicia. (27 de Enero de 2010). *Sentencia 1668-10.* Recuperado el 30 de Abril de 2014, de Página web del Poder Judicial: http://sitios.poder-judicial.go.cr/salaconstitucional/Constitucion%20Politica/Sentencias/2010/10-01668.htm

Sala Constitucional de la Corte Suprema de Justicia. (01 de Marzo de 2011). *Voto 2011002638.* Recuperado el 15 de Mayo de 2014, de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/normas/nrm_texto_completo.aspx?param2=1&nValor1=1&nValor2=76290&nValor3=95202&nValor4=NO&strTipM=TC

Sala Constitucional de la Corte Suprema de Justicia. (01 de Marzo de 2011). *Voto 2638-2011.* Recuperado el 15 de Mayo de 2014, de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/normas/nrm_texto_completo.aspx?param2=1&nValor1=1&nValor2=76290&nValor3=95202&nValor4=NO&strTipM=TC

Sala Constitucional de la Corte Suprema de Justicia. (19 de Noviembre de 2013). *Sentencia Nº 2013-15183.* Recuperado el 12 de Marzo de 2014, de Sistema Costarricense de Información Jurídica:

http://200.91.68.20/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=593984&strTipM=T&strDirSel=directo

Santos Morón, M. J. (2011). *Menores y derechos de la personalidad. Autonomía del menor.* Recuperado el 05 de enero de 2013, de Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid: http://www.uam.es/otros/afduam/pdf/15/M%20J%20Santos.pdf

Sarra, A. V. (2001). *Comercio electrónico y derecho, aspectos jurídicos de los negocios en internet.* Buenos Aires: Astrea.

Seminario Internet y Sistema Judicial. (9 de Julio de 2003). *Reglas de Heredia: Reglas mínimas para la difusión de información judicial en Internet.* Recuperado el 01 de Marzo de 2014, de Página web de María Silvia Villaverde: http://www.villaverde.com.ar/es/assets/novedades/varios/018-reglas-heredia.doc

Shanahan, F. (Marzo de 2008). *Mapa de la Fragmentación de la Identidad en Internet.* Recuperado el 24 de Marzo de 2014, de identite-numerique.fr: http://www.identite-numerique.fr/wp-content/uploads/2008/03/identityfrag.png

Shane, S., & Somaiya, R. (16 de Junio de 2013). *New leak indicates U.S. and Britain eavesdropped at '09 world conferences.* Recuperado el 04 de Agosto de 2013, de The New York Times: http://www.nytimes.com/2013/06/17/world/europe/new-leak-indicates-us-and-britain-eavesdropped-at-09-world-conferences.html

Siriram, R. (Mayo de 2011). Convergence of Technologies. *South African Journal of Industrial Engineering, Vol 22*(1), 13-27.

Skelsey, A. (2002). *Packet Switching.* Recuperado el 21 de Diciembre de 2013, de Communication Networks, University of Technology, Sydney: http://services.eng.uts.edu.au/~kumbes/ra/Switching/Packet-Switching/packet.html

Solano Chaves, Y. (2012). *El delito de Fraude de Simulación en la sociedad costarricense frente a la revolución informática y tecnológica. Trabajo final de graduación para optar por el grado de licenciatura en Derecho.* San José: Universidad de Costa Rica.

Solorio Pérez, O. J. (27 de Marzo de 2009). *Presentación: Módulo III. Habeas data y supuestos de reserva de información pública 3. Principios de Protección de Datos.* Recuperado el 16 de Abril de 2013, de Página web del Instituto de Transparencia e Información Pública del Estado de Jalisco: http://www.itei.org.mx/v3/micrositios/interinstitucional/presentaciones/oscarjsolorio_27_28_marzo_09.pdf

Soro Russell, O. (2007). *El principio de la autonomía de la voluntad privada en lacontratación: Génesis y contenido actual.* Recuperado el 25 de Febrero de 2013, de Página web de la Universidad Complutense de Madrid: http://eprints.ucm.es/12205/2/DEA_El_principio_de_la_autonom%C3%ADa_de_la_voluntad_privada_en_la_contratacion.pdf

Soto Vega, F. (2011). *Uso consentido de información personal en contratos comerciales de adhesión en Costa Rica. Trabajo final de graduación para optar por el título de licenciatura en Derecho.* San José: Universidad de Costa Rica.

Standage, T. (Octubre de 2001). The Internet, Undeterred. *The Economist*, p. 16.

Stieglitz, E. J. (2007). Notes & Recent Development: Anonymity on the Internet: How Does It Work, Who Needs It, and What are Its Policy Implications? *China Law Digest*, 1395-1417.

Stonebruner, G., Hayden, C., & Feringa, A. (Junio de 2004). *Engineering Principles for Information Security (A Baseline for Achieving Security), revision A.* Recuperado el 13 de Abril de 2013, de National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

Suárez Crothers, C. (2001). *Transferencia de datos personales a países terceros y el caso de internet.* Recuperado el 06 de Mayo de 2013, de Ius et Praxis v.7 n.2: http://www.scielo.cl/scielo.php?pid=S0718-00122001000200014&script=sci_arttext

Suñé Llinás, E. (Diciembre de 2006). *Del derecho informático al derecho del ciberespacio y a la constitución del ciberespacio.* Recuperado el 10 de Abril de 2013, de Iuris Tantum, vlex.com: http://doctrina.vlex.com.mx/vid/informatico-ciberespacio-54803677

Superintendencia de Telecomunicaciones. (2010). *Informe del Sector de Telecomunicaciones 2010.* Recuperado el 19 de Diciembre de 2013, de www.amcham.co.cr: http://www.amcham.co.cr/newsletters/201002/telecom.pdf

Superintendencia de Telecomunicaciones. (19 de Diciembre de 2012). *Acuerdo 014-077-2012 SUTEL sobre Procedimiento de Comunicaciones no Solicitadas.* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74081&nValor3=91192&strTipM=TC

Superintendencia de Telecomunicaciones. (22 de Agosto de 2012). *Resolución RCS-251-2012.* Recuperado el 20 de Febrero de 2014, de infocom.cr: http://www.infocom.cr/downloads/docs/Documentos para consulta/Resolución RCS-251-2012 Sistema de Emergencias 9-1-1.pdf

Superintendencia de Telecomunicaciones. (10 de Octubre de 2012). *Resolución RCS-303-2012 "Disposiciones complementarias, técnicas, económicas y administrativas para la implementación y operación del sistema integral de portalidad numérica en Costa Rica".* Recuperado el 01 de Mayo de 2014, de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73777&nValor3=92843&strTipM=TC

Superintendencia de Telecomunicaciones. (22 de Noviembre de 2013). *Autorizados por Sutel para brindar servicios de telecomunicaciones.* Recuperado el 03 de Enero de 2014, de

Registro Nacional de Telecomunicaciones: https://docs.google.com/viewer?a=v&pid=sites&srcid=cm50LnN1dGVsLmdvLmNyfHJudHxneDoxZjUwODAxYTU5YmRiNjRk

Superintendencia de Telecomunicaciones de Costa Rica. (Agosto de 2009). *Determinación de los mercados relevantes y los operadores o proveedores importantes.* Recuperado el 03 de Mayo de 2011, de Página web de la Superintendencia de Telecomunicaciones de Costa Rica: http://www.expotelecom.net/documentos/propuesta_mercados_relevantesSUTEL.pdf

Swire, P. P. (Febrero de 1998). *Avoiding a Showdown Over EU Privacy Laws.* Recuperado el 18 de Enero de 2012, de The Brookings Institution: www.brookings.edu/papers/1998/02europe_swire.aspx

Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks (Fourth Edition).* New Jersey: Prentice Hall.

Téllez Valdés, J. (2003). *Derecho Informático.* México: Mc Graw Hill.

Terrón Santos, D. (Septiembre de 2005). Cinco regulaciones para una misma realidad: la protección de datos en las comunicaciones electrónicas. *Revista del Derecho de las Telecomunicaciones e Infraestructuras en Red - Núm. 24, Septiembre 2005*(24), págs. 47-62.

The 3M Company. (2011). *Marco Regulatorio de la Protección de Datos en Argentina.* Recuperado el 06 de Septiembre de 2013, de Página web de 3M Argentina: http://solutions.3m.com.ar/3MContentRetrievalAPI/BlobServlet?lmd=1342730169000&locale=es_AR&assetType=MMM_Image&assetId=1319233947701&blobAttribute=ImageFile

The Consumer Energy Council of America Convergence Forum. (Abril de 2000). *The Convergence Phenomenon: A Consumer Perspective.* Washington DC: The Consumer Energy Council of America.

The White House. (Febrero de 2012). *Consumer Data Privacy in a Networked World: A framework for protecting privacy and promoting innovation in the global digital economy.* Recuperado el 31 de Agosto de 2013, de whitehouse.gob: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Thierer, A. (2003). *Who Rules the Net?: Internet Governance and Jurisdiction.* Washington DC: Instituto CATO / National Book Network.

Torres, J. L. (Enero-Junio de 2002). Naturaleza e historia de los Derechos Humanos. *Revista Espiga, Escuela de Ciencias Sociales y Humanidades, Universidad Estatal a Distancia de Costa Rica*, 1-14.

Traña Porras, N. (2008). *Un marco regulatorio para las telecomunicaciones en el mercado de apertura: Armonización con la normativa internacional, Trabajo final de graduación para optar al grado de licenciatura en Derecho.* San José: Universidad de Costa Rica.

Tribunal Constitucional de la República del Perú . (10 de Abril de 2003). *00700-2003-HC/TC Lima.* Recuperado el 06 de Septiembre de 2013, de Vlex Jurisprudencia Perú: http://vlex.com.pe/vid/-387565964

Tribunal Constitucional de la República del Perú. (1996). *Sentencia 00666-1996-HD.* Recuperado el 06 de Septiembre de 2013, de Página web del Tribunal Constitucional de la República del Perú: http://www.tc.gob.pe/jurisprudencia/1998/00666-1996-HD.html

Tribunal Constitucional Peruano. (21 de Diciembre de 2007). *Sentencia 06164-2007-HD/TC.* Recuperado el 15 de Abril de 2014, de Página web del Tribunal Constitucional: http://www.tc.gob.pe/jurisprudencia/2008/06164-2007-HD.html

Tribunal Superior de Justicia de Brasil. (2010). *Alexandre Magno Silva Marangon v Google Brasil Internet Ltda - Relatório e Voto.* Recuperado el 04 de Septiembre de 2013, de jusBrasil: http://stj.jusbrasil.com.br/jurisprudencia/21078237/recurso-especial-resp-1186616-mg-2010-0051226-3-stj/relatorio-e-voto-21078239

Tsai, J. Y., Gage Kelley, P., Faith Cranor, L., & Sadeh, N. (Febreri de 2010). *Location-sharing technologies: Privacy risks and controls.* Recuperado el 18 de Mayo de 2013, de Página web del Cylab Usable Privacy and Security Laboratory: http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf

U.S. Department of Health & Human Services. (2013). *Summary of the HIPAA Privacy Rule.* Recuperado el 29 de Agosto de 2013, de Health Information Privacy: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

Unión Europea. (09 de Mayo de 2008). *Versión Consolidada del Tratado de la Unión Europea.* Recuperado el 04 de Junio de 2013, de Diario Oficial de la Unión Europea - Página web oficial de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:019:es:PDF

Unión Europea. (30 de Marzo de 2010). *Versión Consolidada del Tratado de Funcionamiento de la Unión Europea.* Recuperado el 15 de Junio de 2013, de Diario Oficial de la Unión Europea - Página web oficial de la Unión Europea: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:es:PDF

Unión Internacional de las Telecomunicaciones. (1989). *International Telecommunication Regulations.* Recuperado el 20 de Enero de 2014, de Página web de la UIT: http://www.itu.int/ITU-T/itr/files/ITR-e.doc

Unión Internacional de las Telecomunicaciones. (2012). *Costa Rica Profile (Latest data available: 2012).* Recuperado el 20 de Diciembre de 2013, de Página web de la ITU: https://www.google.com/url?q=http://www.itu.int/net4/itu-

d/icteye/CountryProfileReport.aspx%3FcountryID%3D62&sa=U&ei=80r3Uuz6J-jgyQHyy4GwAw&ved=0CAwQFjAGOAo&client=internal-uds-cse&usg=AFQjCNGm50cX-MixYVNV2yFBnYSspW9oLQ

Unión Internacional de Telecomunicaciones. (2004). *Principios y requisitos para la convergencia de sistemas fijos e IMT-2000 existentes - Recomendación UIT-T Q-1761.* Recuperado el 28 de Octubre de 2013, de Página web de la UIT: http://www.itu.int/rec/T-REC-Q.1761/es

Unión Internacional de Telecomunicaciones. (2010). *Decisiones destacadas de Guadalajara - Ciberseguridad*. Recuperado el 11 de Abril de 2013, de Actualidades de la UIT: http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

United Nations Conference on Trade and Development. (2010). *Study on prospects for harmonizing cyberlegislation in Latin America.* Recuperado el 28 de Abril de 2014, de Página web de las Naciones Unidas: http://unctad.org/en/docs/dtlstict20091_en.pdf

United Nations Development Programme. (2013). *Informe sobre desarrollo humano 2013 El ascenso del Sur: Progreso humano en un mundo diverso.* Recuperado el 13 de Enero de 2014, de Página web del programa de las Naciones Unidas para el Desarrollo: http://www.pnud.org.ec/Noticias2013/HDR2013%20Report%20Spanish.pdf

United States Environmental Protection Agency. (19 de Enero de 2013). *Frequent Questions - Privacy Act.* Recuperado el 28 de Agosto de 2013, de Página web de la U.S. Environmental Protection Agency: http://epa.gov/privacy/faqs/index.htm

University of Virginia. (2013). *FERPA: An introduction to the family educational rights and privacy act.* Recuperado el 29 de Agosto de 2013, de University of Virginia, registrar: http://www.virginia.edu/registrar/documents/FERPA.pdf

Valladares Lanza, L. (2008). *Elementos para una conceptualización del Derecho a la Información.* Recuperado el 10 de Marzo de 2013, de Página web del Consejo Nacional Anticorrupción de Honduras: http://www.cna.hn/archivos/coleccion_etica/elementos_conceptualizacion.pdf

Vázquez Bote, E. (septiembre de 1973). *Los denominados derechos de la personalidad.* Recuperado el 09 de enero de 2013, de Biblioteca Jurídica Virtual - UNAM - Boletín Mexicano de Derecho Comparado: http://biblio.juridicas.unam.mx/revista/pdf/DerechoComparado/18/art/art3.pdf

Veillette, C. (10 de Febrero de 2005). *Costa Rica: Background and U.S. relations.* Recuperado el 13 de Enero de 2014, de Página web del Departamento de Estado de los Estados Unidos de América: http://fpc.state.gov/documents/organization/47152.pdf

Veleiro Reboredo, B. (2008). *Protección de datos de carácter personal y Sociedad de la Información.* Madrid: Boletín Oficial del Estado.

Veljanovich, R. D. (1997). *El derecho a la información y las cláusulas protectoras del ejercicio profesional. La cláúsula de consciencia y el secreto profesional del periodista.* Recuperado el 10 de Marzo de 2013, de Página web de la Universidad de Buenos Aires: http://www.catedras.fsoc.uba.ar/loreti/documentos_de_la_catedra/veljanovich_002.pdf

Villalobos Quirós, E. (1997). *El derecho a la información.* San José: Euned.

Warren, A., Dearnley, J., & Oppenheim, C. (2001). *Sources of Literature on Data Protection and Human Rights.* Recuperado el 27 de Marzo de 2012, de Electronic Law Journals, Warwick University: www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_2/warren/

Westin, A. (1967). *Privacy and Freedom.* New York: Atheneum.

Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality.* New York: The New Press.

Whitman, M. E., & Mattford, H. J. (2012). *Principles of Information Security, Fourth Edition (extracto)*. Recuperado el 13 de Abril de 2013, de Página web de Cengage learning: http://www.cengagebrain.com/content/whitman38214_1111138214_01.01_toc.pdf

Winton, A., Zhang, A., Innes-Stubb, S., & Xu, L. (Marzo de 2012). *Data protection and privacy in China.* Recuperado el 05 de Octubre de 2013, de Página web de White & Case: http://www.whitecase.com/files/Publication/58829ab4-e10d-4371-b722-74681b4ac7e6/Presentation/PublicationAttachment/07ca803c-6ce8-49ae-8b4d-622557551990/alert-Data-Protection-and-Privacy-in%20China-March-2012.pdf

World Economic Forum. (Enero de 2011). *Personal Data: the emergence of a new asset class.* Recuperado el 17 de Abril de 2013, de Página web del World Economic Forum: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

World Economic Forum. (Mayo de 2012). *Rethinking personal data: strenghtening trust.* Recuperado el 17 de Abril de 2013, de Página web del World Economic Forum: http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf

World Economic Forum. (Febrero de 2013). *Unlocking the value of personal data: from collection to usage.* Recuperado el 17 de Abril de 2013, de Página web del World Economic Forum: http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. (15 de Noviembre de 2003). *Declaración de Santa Cruz de la Sierra (Bolivia): "La inclusión social, motor del desarrollo de la Comunidad Iberoamericana".* Recuperado el 04 de Marzo de 2014, de Página web de la Organización de Estados Iberoamericanos: http://www.oei.es/xiiicumbredec.htm

XIV Cumbre Judicial Iberoamericana. (8 de Marzo de 2008). *100 Reglas de Brasilia sobre acceso a la justicia de las personas en condición de vulnerabilidad.* Recuperado el 2 de Marzo de 2014, de Página web de la secretaría permanente de la Cumbre Judicial Iberoamericana: http://www.cumbrejudicial.org/c/document_library/get_file?uuid=10cef78a-d983-4202-816e-3ee95d9c1c3f&groupId=10124

Yang, Ming; Ranzato, Marc' Aurelio; Wolf, Lior. (11 de Marzo de 2014). *Deep face: closing the gap to human-level performance in face verification.* Recuperado el 27 de Marzo de 2014, de Página web de la Universidad de Illinois: http://www.cs.tau.ac.il/~wolf/papers/deepface.pdf

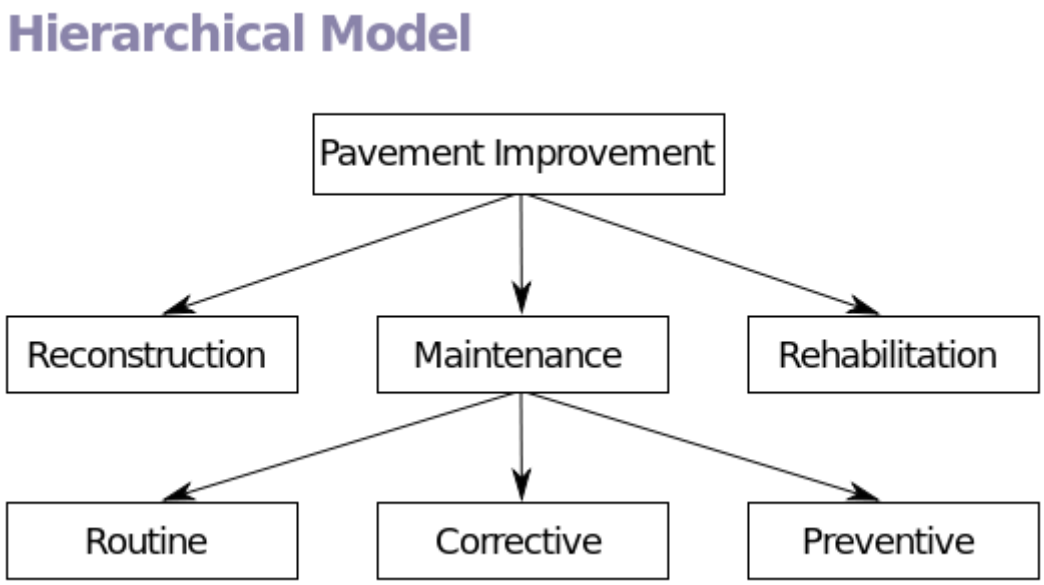
Zamora Hernández, C. (11 de septiembre de 2007). *Violación de los derechos de los menores de edad en un conflicto armado.* Recuperado el 21 de enero de 2012, de Colección de tesis digitales Universidad de las Américas Puebla: http://catarina.udlap.mx/u_dl_a/tales/documentos/ledi/zamora_h_ck/portada.html

Zimmerman, R. K. (2001). *The way the "cookies" crumble: Internet privacy and data protection in the twenty-first century.* Recuperado el 15 de Mayo de 2013, de New York University Journal of Legislation and Public Policy: http://www.law.nyu.edu/ecm_dlv/groups/public/@nyu_law_website__journals__journal_of_legislation_and_public_policy/documents/documents/ecm_pro_060646.pdf

# Anexos

## Anexo 1

Ejemplo del modelo jerárquico de gestión de bases de datos. (Departamento de Transporte de Estados Unidos, 2001)



## Anexo 2

Ejemplo del modelo relacional de gestión de bases de datos. (Departamento de Transporte de Estados Unidos, 2001).

### Relational Model

| Activity Code | Activity Name |
|---|---|
| 23 | Patching |
| 24 | Overlay |
| 25 | Crack Sealing |

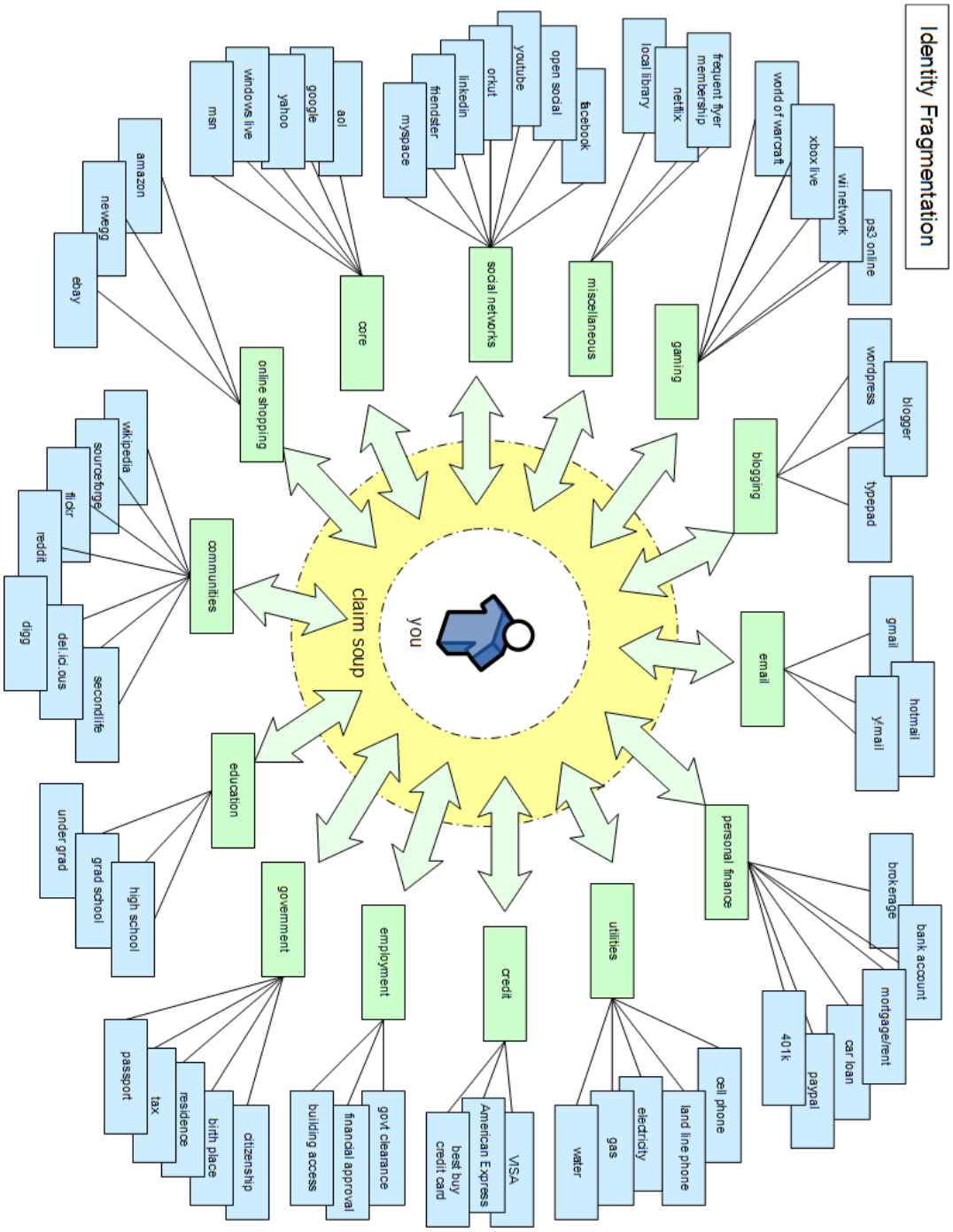
Key = 24

| Activity Code | Date | Route No. |
|---|---|---|
| 24 | 01/12/01 | I-95 |
| 24 | 02/08/01 | I-66 |

| Date | Activity Code | Route No. |
|---|---|---|
| 01/12/01 | 24 | I-95 |
| 01/15/01 | 23 | I-495 |
| 02/08/01 | 24 | I-66 |

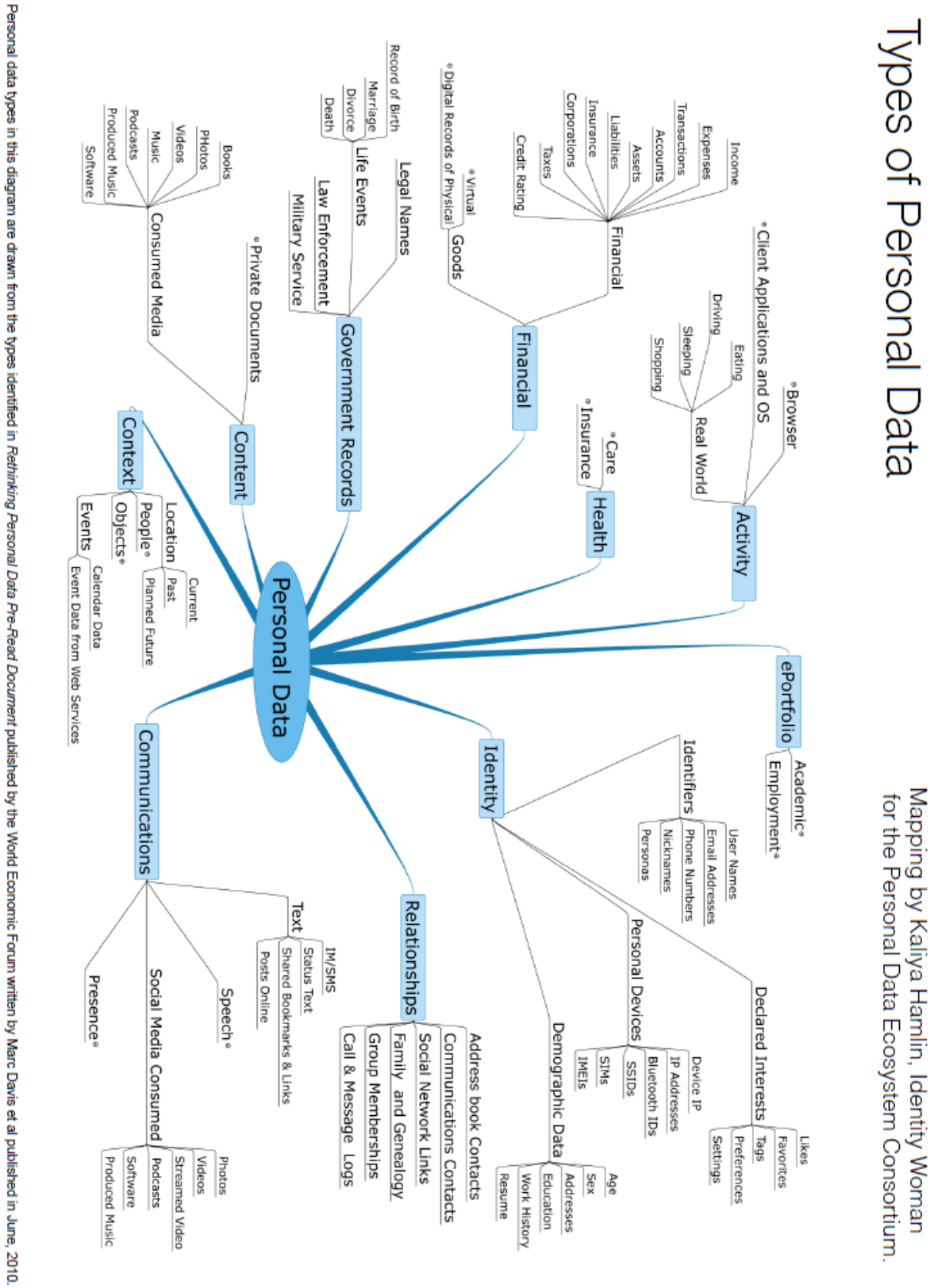
## Anexo 3

Imagen representativa de la fragmentación de las manifestaciones de la personalidad o identidad virtual de una persona (Shanahan, 2008).



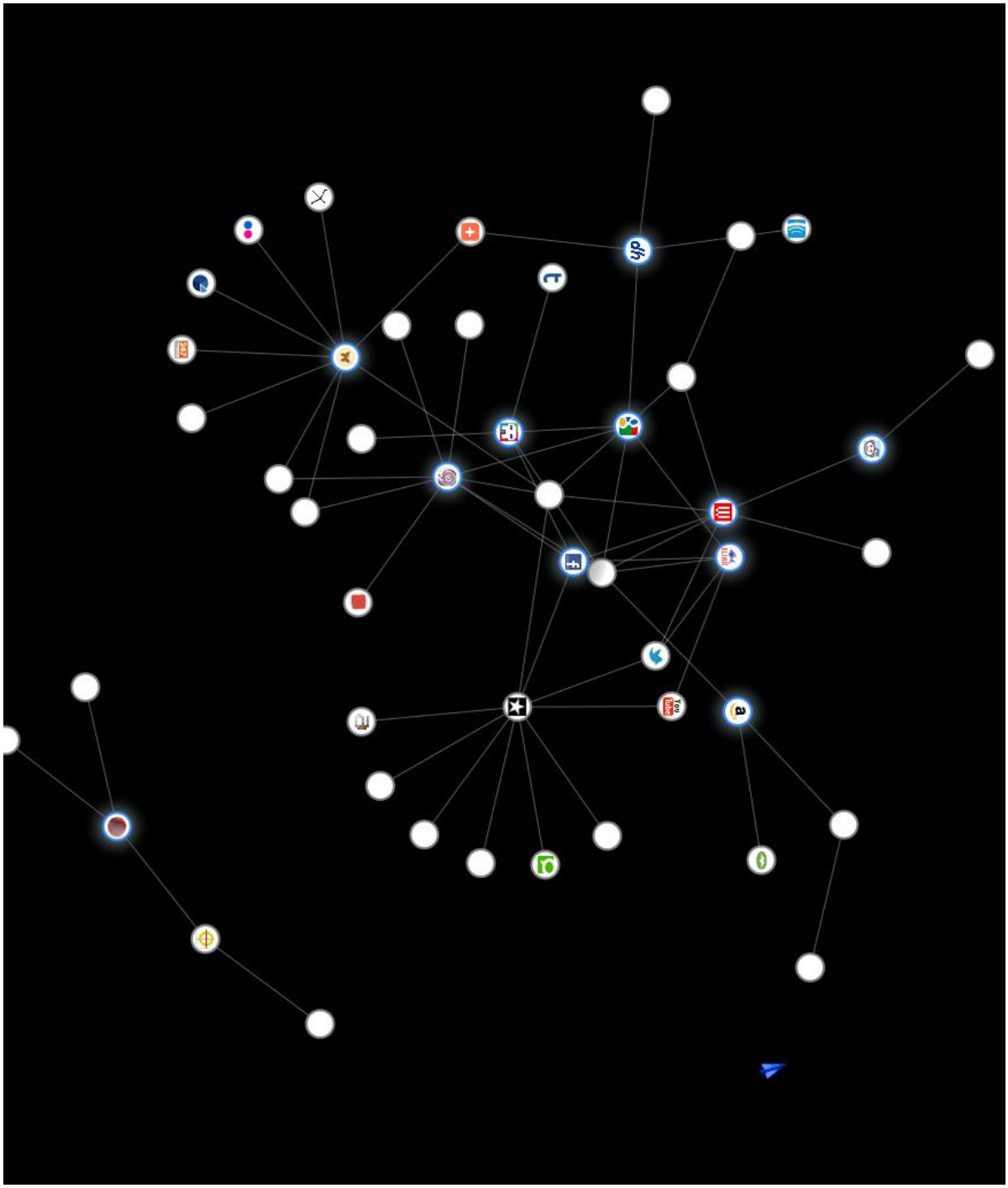
## Anexo 4

Mapa de los tipos de datos personales (Hamlin, 2011).



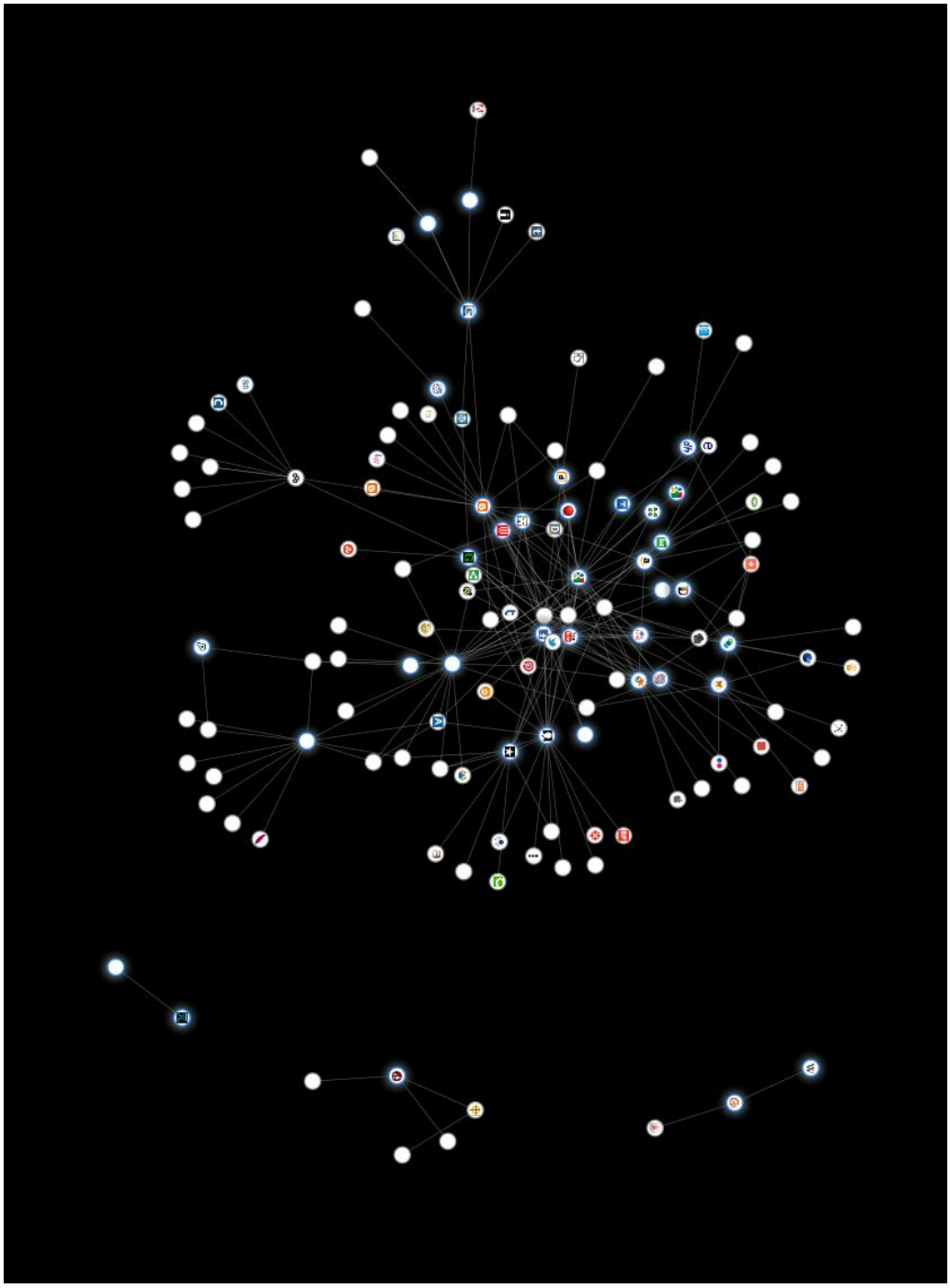
## Anexo 5

Resultados gráficos producidos el 26 de octubre de 2011 por la aplicación *Collusion* tras 5 minutos de ser admitido el uso de *cookies* en un navegador de internet.



## Anexo 6

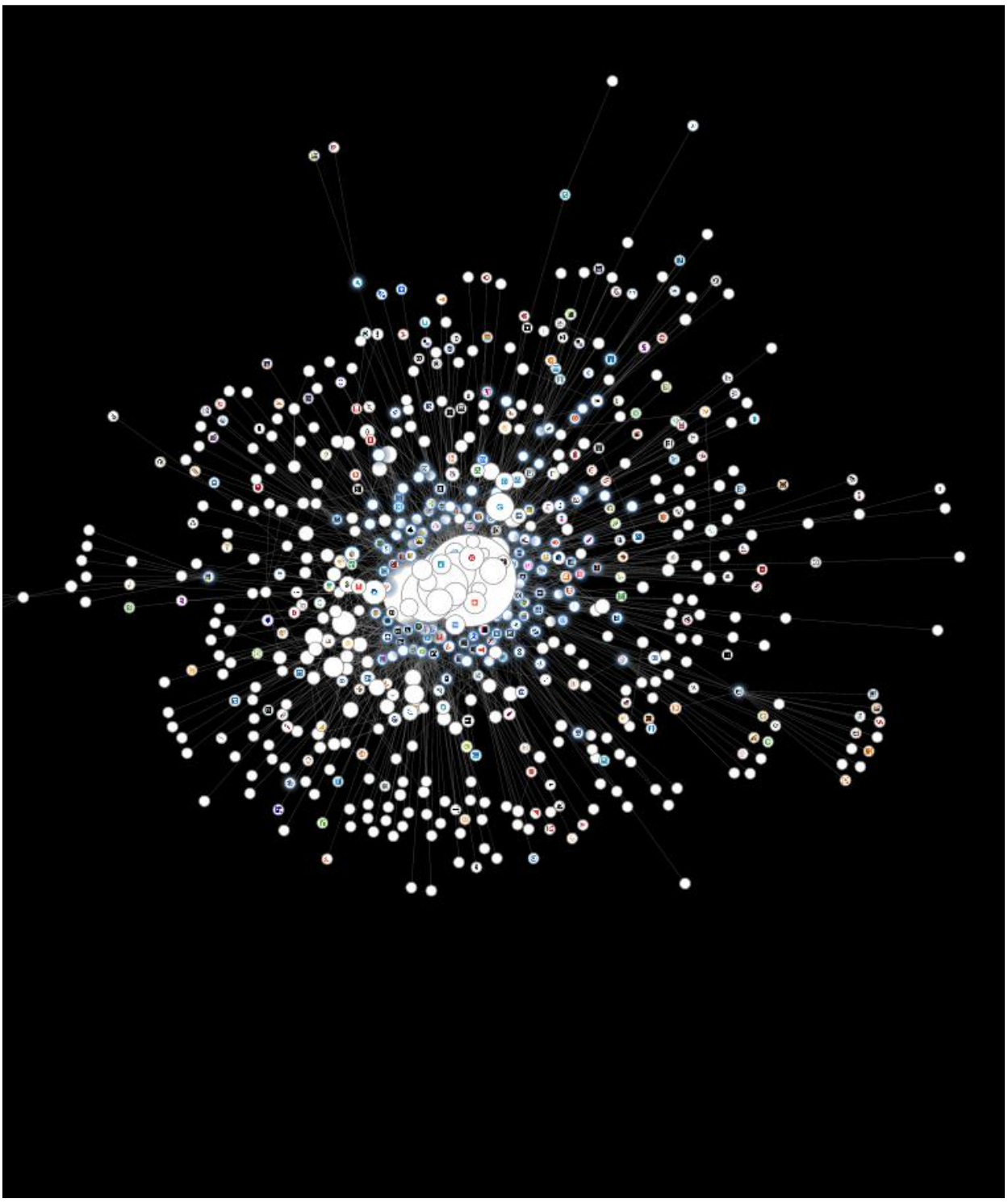
Resultados gráficos producidos el 26 de octubre de 2011 por la aplicación Collusion en el que se muestran las páginas visitadas a lo largo del día y aquellas que rastrean nuestro paso por Internet por medio de cookies.



## Anexo 7

Resultados gráficos producidos el 08 de noviembre de 2012 tras un año sin borrar las cookies del navegador de internet. En él se muestran las páginas visitadas a lo largo del año y aquellas que han rastreado nuestro paso por Internet por medio de cookies. Debe resaltarse que para este punto la nube se encuentra tan llena de interrelaciones que es necesario alejar totalmente el zoom para poder observar su totalidad, por lo que es imposible observar mayores detalles en el centro de esta.

Asimismo debe resaltarse que para este momento ya se denotan ciertas burbujas grises (páginas rastreadoras) que han crecido exponencialmente, lo cual significa que estas se encuentran conectadas a un número mayor de páginas visitadas.

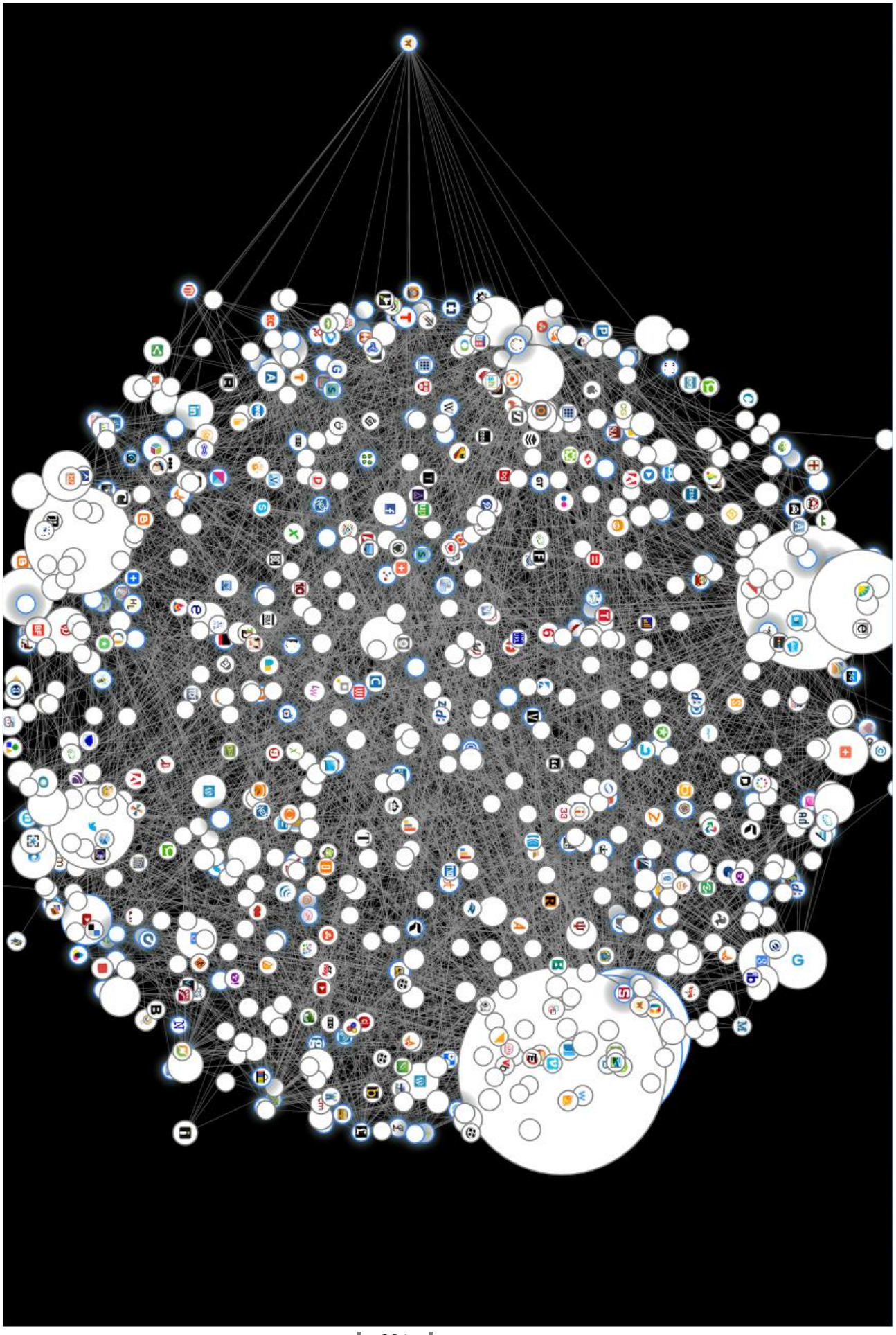


## Anexo 8

Resultados gráficos producidos el 10 de abril de 2013 tras dieciocho meses sin borrar las cookies del navegador de internet. En este último ejemplo se puede observar cómo la nube de interrelaciones se ha ampliado al punto de que absorbe la imagen entera (la vista presentada representa el máximo nivel de alejamiento permitido por el programa), por lo que resulta imposible determinar los detalles específicos de las páginas encontradas en los puntos de convergencia de las líneas grises.

Nuevamente es posible identificar también cómo las páginas más visitadas por el usuario se mantienen aún visibles, siendo siempre superadas en tamaño por un buen número de páginas rastreadoras que, para este momento, cuentan probablemente con un perfil certero del usuario.

Esta imagen representó el final de la investigación realizada en materia de rastreo por cookies, pues para ese momento la cantidad de información acumulada resultaba tan grande que su tratamiento y graficación por la aplicación absorbía por completo el hardware informático utilizado.



## Anexo 9

Parte de la respuesta brindada por el Departamento de Estado de los Estados Unidos a epic.org, frente a su solicitud de acceso a la información con referencia al caso de compra de datos de ciudadanos latinoamericanos bajo la Freedom of Information Act. (Departamento de Estado de los Estados Unidos de América, 2003).

United States Department of State

*Washington, D.C. 20520*

NOV - 3 2003

Case No. 200301593
Segment No. SANJO001

Mr. Chris Hoofnagle
Deputy Counsel
**epic.org**
1718 Connecticut Ave., NW
Suite 200
Washington DC 20009

Dear Mr. Hoofnagle:

I refer to your request of May 8, 2003, and June 23, 2003, for the release of information under the Freedom of Information Act (Title 5 USC Section 552). To retrieve the documents you requested we initiated a search of the following record systems under the control of the Department of State: the Central Foreign Policy Records (the Department's principal record system), the American Embassy in Bogota, the American Embassy in Managua, the American Embassy in San Jose, the American Embassy in San Salvador, the American Embassy in Tegucigalpa, the American Embassy in Brasilia, the American Embassy in Buenos Aires, the American Embassy in Caracas, the American Embassy in Guatemala City, and the American Embassy in Mexico City.

The search of the records of the American Embassy in San Jose has been completed, resulting in the retrieval of eleven documents that appear responsive to your request. After reviewing these documents, we have determined that all may be released in full. All released material is enclosed.

The searches of the records of the American Embassy in San Salvador, the American Embassy in Tegucigalpa, the American Embassy in Buenos Aires, and the American Embassy in Caracas have also been completed, resulting in the retrieval of no documents responsive to your request.

In addition, the search of the records of the Central Foreign Policy Records has been completed, resulting in the retrieval

of material that may be responsive to your request; that material is currently under review.

Still in progress are the searches of the records of the American Embassy in Bogota, the American Embassy in Managua, the American Embassy in Brasilia, the American Embassy in Guatemala City, and the American Embassy in Mexico City.

Additional information will be provided as soon as it becomes available.

If you have any questions with respect to the processing of your request, you may write to the Office of IRM Programs and Services, SA-2, Department of State, Washington, D.C. 20522-6001. You may also reach us by telephone at (202) 261-8314. Please be sure to refer to the case and segment numbers shown above in all correspondence about this case.

Your continuing cooperation is appreciated.

Sincerely,

Margaret P. Grafeld
Director
Office of IRM Programs and Services

Enclosures:
As stated.

UNCLASSIFIED

La Nación
RELEASED IN FULL

UNITED STATES DEPARTMENT OF STATE
REVIEW AUTHORITY: OSCAR J OLSON
DATE/CASE ID: 23 OCT 2003 200301593

4
LA NACIÓN, MIÉRCOLES 6 DE AGOSTO DEL 2003

ELPAÍS

Coordinador de Política Carlos Villalobos. cvilla@nacion.com

INFORME DE COMISIÓN QUE NOMBRÓ EL GOBIERNO

# Presumen que hay venta de datos del ICE, MOPT y Caja

## Consejo pide al Ministerio Público ahondar pesquisa

BERLIOTH HERRERA
bherrera@nacion.com

Empresas que se dedican a vender información de los ciudadanos podrían estar obteniendo, ilegalmente, datos privados de las bases del ICE, el MOPT y la Caja Costarricense de Seguro Social (CCSS).

La presunción la planteó una comisión interinstitucional que investigó el asunto. Su informe fue conocido y aprobado ayer por el Consejo de Gobierno, que acordó remitirlo al Ministerio Público para que investigue la sospecha.

En el documento, el grupo señaló que, además de la información que las empresas dedicadas a ese negocio obtienen de las bases de datos del Registro Público y el Registro de la Propiedad, también

Informe completo en www.nacion.com

se presume que la están adquiriendo ilegalmente del Instituto Costarricense de Electricidad, la Caja Costarricense de Seguro Social y el Ministerio de Obras Públicas y Transportes (MOPT).

"Prueba de ello –agregó– es que las empresas en cuestión mantienen actualizada la información que venden relacionada con patrono para el que labora (anteriores y actual), salarios y fechas de los cambios de los mismos, entre otros".

El Gobierno ordenó la investigación en abril cuando trascendió que empresas estadounidenses que se dedican a tal negocio –como ChoicePoint– confirmaron que compraban archivos a subcontratistas en 10 países latinoamericanos, entre ellos Costa Rica.

De acuerdo con la información suministrada por el Gobierno, la Oficina Federal de Investigaciones (FBI) le comunicó que actualmente no se accede a información de costarricenses a través de ChoicePoint.

El informe lo elaboraron representantes de los ministerios de Justicia y de Seguridad Pública, el Poder Judicial, el Consejo de Seguridad Integral, el Ministerio Público, la Dirección de Inteligencia y Seguridad (DIS) y la Procuraduría General de la República.

### Acceso a lo privado

Igualmente cuestionó el hecho de que las empresas dedicadas a vender datos pueden suministrar números de teléfonos privados –celulares y residenciales–.

Esto "pese a que el abonado del ICE paga un monto adicional para que sus números no aparezcan en los identificadores de llamadas ni en la guía telefónica".

Otro punto que llamó la atención del Gobierno es que las firmas comercializadoras de datos tengan acceso a las bases del MOPT "que contienen las fotografías de las licencias de conducir".

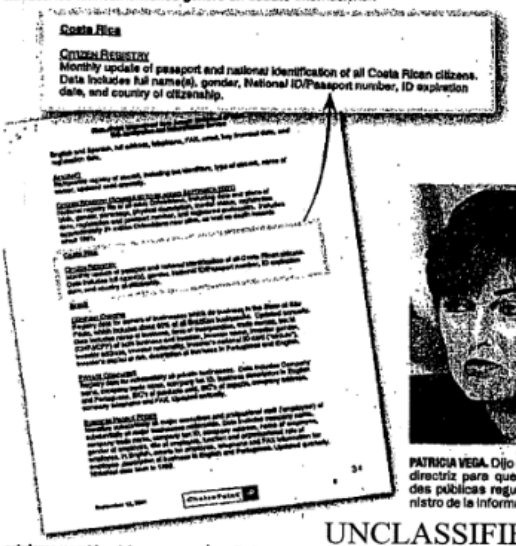
El ministro de Seguridad, Rogelio Ramos, dijo que se decidió remitir el informe al Ministerio Público porque "es necesario" determinar cómo se adquirió información que está protegida por algún tipo de normativa.

Ayer no se pudo hablar con el titular del MOPT, Javier Chaves; con el presidente ejecutivo de la CCSS, Eliseo Vargas, ni con el subgerente de Telecomunicaciones del ICE, Álvaro Retana.

Entre tanto, el gerente de la empresa Datum.net, Rodrigo Mora, insistió ayer en que la firma obtiene la información de fuentes públicas y legales, y que su tarea es ordenarla.

### DESTAPE DE INFORMACIÓN

La noticia de que el Gobierno estadounidense adquiría información de empresas privadas sobre ciudadanos latinoamericanos generó un debate internacional.






ARCHIVO / LA NACIÓN

**PATRICIA VEGA.** Dijo que giró una directriz para que las entidades públicas regulen el suministro de la información.

### MEJORAR LEGISLACIÓN

Piden a diputados agilizar trámite para nueva ley

El Gobierno pidió ayer a los diputados que agilicen el trámite de una nueva normativa que permita proteger la privacidad de los ciudadanos.

Señaló que la ausencia de la normativa pertinente "pone en peligro los derechos constitucionales". Por ello, convocará tres proyectos de ley para que los diputados los conozcan durante el período de sesiones extraordinarias.

Se trata de dos iniciativas que procuran adicionar un nuevo capítulo denominado **Hábeas Data**, al título III de la *Ley de la Jurisdicción Constitucional*.

Uno de estos planes busca, además, que se establezca el secreto de Estado.

El tercer proyecto que convocará el Ejecutivo propone crear una agencia pública de protección de datos.

Sería un ente gubernamental que concentre toda la información de los ciudadanos y vele por el buen uso de la información.

También establece sanciones para quienes violenten esta normativa.

**La ministra de Justicia, Patricia Vega, pidió a los legisladores que le den un trámite ágil a la legislación.**

Laura Chinchilla, diputada liberacionista, dijo que considera que hay ambiente para discutir este tema en cuanto se convoquen los planes.

El legislador Federico Malavassi, del Movimiento Libertario, advirtió que el problema se podría suscitar si tratan de complicar los planes.

"Hay quienes quieren además poner frenos a todo tipo de acceso a la información", dijo.

UNCLASSIFIED

## ChoicePoint activó la alerta en el país

BERLIOTH HERRERA
bherrera@nacion.com

La posible venta de información personal de costarricenses al Gobierno de Estados Unidos fue lo que llevó al Poder Ejecutivo a abrir una investigación sobre la comercialización de ese tipo de datos.

En abril, la empresa estadounidense ChoicePoint confirmó que estaba comprando archivos con información de ciudadanos a subcontratistas en diez países latinoamericanos, entre los cuales figuraba Costa Rica.

De acuerdo con la información que trascendió en ese momento, el Gobierno de Estados Unidos obtenía información personal de extranjeros, especialmente de aquellos que intentan entrar a ese país.

Las dos grandes empresas norteamericanas que se dedican a ese negocio son ChoicePoint y LexisNexis.


ARCHIVO / LA NACIÓN

**DESDE ALLÍ.** La empresa ChoicePoint tiene su sede en el estado norteamericano de Georgia, en el sureste de la nación.

Ayer, cuando se conoció el informe de la comisión que constituyó el Gobierno, se dijo que a través de ChoicePoint no se obtenía actualmente información de los costarricenses.

No obstante, hace poco tiempo, en su página en la red Internet, esa empresa publicitaba la obtención de información de ciudadanos de Costa Rica, entre otras naciones.

¡VIVAN SIEMPRE EL TRABAJO Y LA PAZ!

# AL Día

Martes 5 de agosto, 2003. San José, Costa Rica.

S2

La mejo... cobertu... del cam... naciona... 2003-20...

PORTADA | NACIONALES | OVACION | SOCIEDAD | USTED OPINA | BUS...

- NACIONALES
- SUCESOS
- OPINION
- SOCIEDAD
- OVACION
- EL NORTE
- INTERNACIONALES
- SERVICIOS
- USTED OPINA
- GALERIA
- PURA VIDA
- ESCRIBANOS

NACIONALES — ENVIAR NOTICIA A UN AMIGO — EDICIONES

Ir a -> ÚLTIMA HORA:

## ÚLTIMA HORA:

*Aspectos más importantes del Consejo de Gobierno:*

Tras el Consejo de Gobierno efectuado esta mañana en Casa Presidencial, el mandatario Abel Pacheco afirmó que, pese al lío desatado por la aparición de cuentas y cheques de su campaña política "olvidados", aún mantiene su confianza en el grupo de personas que se encargaron de las finanzas.


"Confío plenamente en la gente que manejó el dinero en la campaña, y creo que el problema entre Rodolfo Montero y Roberto Tovar (Canciller) puede resolverse hablando, confío plenamente en ambos, los dos son intachables", manifestó. En entrevista con Al Día el sábado Montero dijo que Tovar era quien "se encargaba de controlar los gastos". El Canciller rechazó esta versión.


El Consejo de la Niñez y de la Adolescencia reiteró la responsabilidad que tienen los padres de proteger a sus hijos, mediante un pronunciamiento extraordinario hecho a partir de la cadena de hechos violentos contra los niños.

La Ministra de la Niñéz, Rosalía Gil, señaló que en los diversos operativos realizados en las calles de San José por el PANI y el Ministerio de Seguridad detectaron padres que llevan a sus hijos a explotarse sexualmente.

El Gobierno presentará un proyecto con reformas legales que limitarían la venta de datos de sus ciudadanos, luego de denuncias de la obtención y venta de información por parte de la empresa estadounidense ChoicePoint, localizada en Georgia, Estados Unidos.

El Día Norte

Esta empresa vendió la información, tanto de costarricenses como de otros países latinoamericanos, al gobierno norteamericano. El Presidente Pacheco y la ministra de Justicia Patricia Vega anunciaron la próxima presentación ante la Asamblea Legislativa del proyecto, así como varias medidas que regirán en tanto no sean aprobadas las reformas.

| PORTADA | NACIONALES | SUCESOS | OPINIÓN | SOCIEDAD | OVACION | EL NORTE |
| INTERNACIONALES | SERVICIOS | USTED OPINA | PURA VIDA | ESCRIBANOS |

· nacion.com. Revista Dominical



UNCLASSIFIED



REVISTA dl DOMINICAL

**Informe especial**

# TIA: el espía más poderoso del mundo

***Ernesto Rivera***
*erivera@nacion.com*

*Un gigantesco sistema de vigilancia recién presentado ante el Congreso de Estados Unidos pretende reunir información personal, telefónica, financiera y médica de toda la población mundial.*

Su nombre clave es TIA (Total Information Awareness) que en inglés significa "Conocimiento total de la información". Fue diseñado por el Comando de Inteligencia Naval de los Estados Unidos como una gigantesca base de datos para almacenar información personal de todas las personas del planeta.

La pretensión del TIA es desmesurada: combinar los últimos desarrollos en informática y la capacidad de localización por satélite con las nuevas tecnologías de identificación de seres humanos a distancia y aplicarlas juntas al espionaje.

Si el proyecto no formara parte de la estrategia oficial de combate al terrorismo del presidente estadounidense George Bush, cualquiera podría pensar que se trata una novela ciencia ficción.

Por ejemplo, mediante una tecnología especial, TIA podrá registrar la forma de caminar (los hábitos motores) de los individuos que tenga bajo investigación y esto permitiría a los agentes de inteligencia buscar y hallar por satélite a esa persona en cualquier lugar del mundo.

**Además:**

- Choicepoint y los espías
- El almirante y su grupo
- Vulnerables

Sin embargo, el proyecto es tan real que, en enero pasado, el senador Ron Wyden (demócrata por Oregón) impulsó una enmienda a la asignación de fondos para el TIA y condicionó la entrega de más dinero (ya han firmado contratos por $93 millones) a que la inteligencia naval suspendiera cualquier indagación contra ciudadanos estadounidenses y entregara al Congreso una descripción completa del proyecto.

Este 20 de mayo, se presentó ante el Congreso de los Estados Unidos un informe sobre TIA.

Mientras los congresistas analizan el informe, la enmienda que protege a los estadounidenses de los ojos



UNCLASSIFIED

## Anexo 10

Nota oficial 9160-AN-273-2012 del Instituto Costarricense de Electricidad en respuesta a solicitud de acceso a la información personal (datos de tráfico y localización) presentada por Adrián Quesada Rodríguez, el 14 de diciembre de 2012.

ICE

27 de diciembre del 2012
9160-AN-273-2012

Sr. Adrián Quesada Rodríguez
Urbanización Las Tres Marías
Naranjo

Asunto: Suministro de información.

En relación a su nota con fecha 14-12-2012, en la cual se solicita información de los datos que el Instituto Costarricense de Electricidad Sector Telecomunicaciones suministra de sus clientes, me permito compartir el criterio legal emitido por la Licda. Guiselle Murillo Cruz de la Dirección Relaciones Regulatorias, División Jurídica Institucional.

La Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, No. 8968 del 7 de julio del 2011, define como datos personales, cualquier dato relativo a una persona física identificada o identificable. De igual forma, así como les otorga definición, para el caso específico de las bases de datos automatizadas que el ICE maneja con sus clientes, también los categoriza en datos personales de acceso restringido, definiéndolos como los datos que aun formando parte de registros de acceso al público, no son de acceso irrestricto o ilimitado, por ser de interés solo para su titular o para la Administración Pública.

En este sentido, tanto la ley de cita en su artículo 7 inciso a) como su reglamento en el artículo 21, señalan el derecho que tiene el titular o persona a obtener del responsable, en este caso del ICE, sin demora y a título gratuito, la confirmación o no de la existencia de información personal en archivos o bases de datos. Estos datos deberán ser comunicados a la persona interesada en forma precisa y entendible.

Conforme lo anterior, la información sensible de los clientes que el ICE guarda en sus bases de datos, son aquellos proporcionados por los propios titulares de los servicios, como son, nombre, cédula, teléfonos de referencia y dirección y, como tales, conforme a la ley, se consideran datos personales de acceso restringido y son utilizados para la prestación del servicio del que se trate.

9160-AN-273-2012
-2-

En cuanto al tiempo de respuesta en que deben atenderse estas peticiones, el mismo es de cinco días hábiles, según se dispone en el artículo 18 del reglamento a la ley No. 8968, y la información solo podrá ser entregada al titular del servicio.

En lo que se refiere a los datos de tráfico de llamadas (entendidas como, listado de llamadas entrantes y salientes), los mismos se deben entregar a su titular, observando la normativa vigente y atendiendo las tarifas aprobadas para este servicio en la resolución RRG-5957-2006 del 1 de agosto del 2006, por tratarse de un servicio regulado al costo, conforme a la Ley No. 8660.

Por último, en lo que respecta a la información requerida sobre las conexiones de datos y las radiobases a las que se conectó el servicio celular, debe indicarse al solicitante, que el ICE no guarda este tipo de registros.

Atentamente,

Lic. William Hernández Araya
Coordinador
Agencia Telefónica de Naranjo

c. Agencia

Apartado postal 10032 San José, Costa Rica
Tel. (506) 2451-7800
Fax (506) 2451-1717
www.grupoice.com