UNIVERSIDAD DE

CASTILLA-LA MANCHA

Facultad de Ciencias Jurídicas y Sociales

ÁREA DE DERECHO CONSTITUCIONAL

TESIS DOCTORAL

PRIVACIDAD EN INTERNET: Los derechos fundamentales de privacidad e intimidad en Internet y su regulación jurídica. La vigilancia masiva.

Presentada por:

ANDRÉS JOSÉ GONZÁLEZ PORRAS

Bajo la dirección del:

Dr. ENRIQUE BELDA PÉREZ-PEDRERO

Toledo, 2015

TÍTULO. PRIVACIDAD EN INTERNET: LOS DERECHOS FUNDAMENTALES DE PRIVACIDAD E INTIMIDAD EN INTERNET Y SU REGULACIÓN JURÍDICA. LA VIGILANCIA MASIVA.

Esta investigación está dedicada la memoria de mi amada madre

Flor Emilia, quien seguro estaría muy orgullosa.

A mi padre Daniel por todo, por sus consejos y apoyos.

A mi esposa e hija, Andrea y Laurita, por su amor y apoyo incondicional.

AGRADECIMIENTOS

Como muchos proyectos de vida, los estudios académicos se plantean como un importante reto, un largo camino que, con el paso del tiempo suele llegar al final. Durante ese agradable recorrido se contó con distintos apoyos y colaboraciones, todas altamente estimadas y necesarias pues, al final de cuentas, de la suma de todas estas dependió la culminación de la investigación.

Indudablemente y, en primer lugar, las gracias a Dios por haberme permitido realizar esta travesía hasta el final. Si bien al inicio las metas parecían inalcanzables Él logró mantener el rumbo y remover todos los obstáculos del camino. Infinitas gracias.

A mis padres pues sin sus ayudas y ejemplo esto no podría ser posible. A mi amada madre Flor Emilia (q.D.g.) quien siempre procuró mi cómoda existencia, estoy seguro que estaría muy orgullosa de poder verme culminar esta etapa de mi vida, por lo que te dedico mi esfuerzo (1953-2015). A mi padre Daniel toda mi gratitud y cariño seguro nunca podré pagarte todo lo que has hecho. Si algún mérito merece este trabajo seguramente es el legado de mis amados padres.

A mi amada esposa, Andrea por su constante apoyo, fuente de mi ánimo y constante inspiración. Mi gratitud por ayudarme a cumplir este sueño. A mi querida hija Laura por su amor incondicional y tantos sacrificios. A mis hermanos Oriana, Daniel, Federico, Paula y familiares por tantas fechas pospuestas y que aún sigan invitándome.

A mis suegros, D. Luis Fernando y D. Yennie infinitas gracias por tanto cariño y compartir de corazón estos sueños, por todas sus colaboraciones y consejos académicos todos muy apreciados.

A todos los compañeros de la Sala Constitucional con quienes he compartido gratos momentos, especialmente a los apreciados compañeros de la oficina

Vanessa, Lil, Laura, Chris, Magaly, Haideer, Jose, Erick, Francisco, Marlyn Andrea y Junior, quienes constantemente me apoyaron. A mis anteriores compañeros de oficina Henry, Vernor, Vilma, Christian y Carlos gracias por haber compartido y por sus incontables discusiones académicas y laborales.

A mis compañeros profesores de la Universidad de Costa Rica Jorge, Isabel, David, Martin, Oscar, Rolando, Carlos por todos sus apoyos en la docencia y la academia. Por haber confiado en los proyectos y brindarme la oportunidad de poder colaborar como docente de ese centro de estudios.

A todos mis amigos, especialmente Alejandro, Navil, José Antonio, José Joaquín, Aarón, Rainier, Gaby, Flora, Mabel y Daniel por su compañía y apoyo, quienes han estado ahí con paciencia en este proceso. A Luis Ricardo y Georgina, por sus colaboraciones académicas y ayudas, verdaderamente importantes en la realización de este trabajo.

A mis alumnos de la Universidad de Costa Rica, Universidad Escuela Libre de Derecho y Universidad Autónoma de Centroamérica con quienes he compartido tan grados momentos y múltiples discusiones académicas las que enriquecen el crecimiento profesional y académico.

A todos mis buenos profesores, aquellos que supieron sembrar ese germen de la investigación, especialmente a los profesores de la Universidad Castilla-La Mancha y al personal administrativo de ese centro de estudios, quienes han sido siempre pacientes y colaboradores.

Al Magistrado Dr. Fernando Cruz Castro, a quien no tengo como agradecer por su constante apoyo e invaluables consejos, sin duda siempre oportunos. Le estaré por siempre agradecido. A todos los demás Magistrados de la Corte Suprema de Justicia que siempre me han apoyado.

Al Profesor Dr. Francisco Javier Díaz Revorio, quien ha sido gran ejemplo por su trayectoria académica y profesional, por todas sus consideraciones y gran estima.

Por último y de forma especial, a mi director y maestro, Dr. Enrique Belda Pérez-Pedrero por su magnánima dedicación en este trabajo de investigación, sus invaluables consejos y guía constante, a quien le debo su infinita paciencia y todas sus consideraciones. En definitiva, por haberme dado ánimo constante, sin el cual seguro no hubiese podido concluir esta etapa académica.

INDICE

TÍTULO. PRIVACIDAD EN INTERNET: Los derechos fundamentales de privacidad e intimidad en Internet y su regulación jurídica. La vigilancia masiva. iii

AGRADECIMIENTOS v

INDICE viii

TABLA DE ABREVIATURAS 14

PRIMERA PARTE. Contextualización del Estudio. 15

CAPÍTULO I. Introducción, Justificación y metodología. 17

1. Abstract. 18
2. Introducción. 20
   - 2.1. Justificación. 27
   - 2.2. Planteamiento de la Investigación. 37
   - 2.3. Alcances y limitaciones. 42
3. Metodología y objetivos. 44
   - 3.1. Metodología. 44
   - 3.2. Objetivo general. 47
   - 3.3. Objetivos específicos. 47

SEGUNDA PARTE. Sobre el Derecho de Intimidad. 49

CAPÍTULO II. La intimidad como valor o concepto. 51

1. Consideraciones preliminares. 52
2. Intimidad y Privacidad, ¿ambas caras de una misma moneda? 54
3. Desarrollo histórico del derecho de privacidad e intimidad. 62
   - 3.1. Origen del concepto de intimidad. 62
   - 3.2. Origen anglosajón del derecho a la *privacy*. 69
   - 3.3. Inicios de la intimidad en Europa. 78
4. Derechos de la sociedad del conocimiento o los derechos de cuarta generación. 87
5. Avance tecnológico y la afectación de los Derechos Humanos. 90

CAPÍTULO III. Naturaleza Jurídica y Contenido del derecho de intimidad. 103

1. Consideraciones preliminares. 104
2. Derecho de Intimidad. 108
   - 2.1. Protección Convencional y Constitucional. 113
     - 2.1.1. La protección convencional. 113
     - 2.1.2. El Derecho de Intimidad en Costa Rica. 120
     - 2.1.3. El Derecho de Intimidad en España. 123
     - 2.1.4. El Derecho de privacidad en EE.UU. 128
   - 2.2. Teorías del derecho de intimidad. 161
     - 2.2.1. Teoría Sphärentheorie (Teoría de las esferas o círculos concéntricos). 161
     - 2.2.2. Teoría del Mosaico. 162
     - 2.2.3. Teoría del “right to privacy”. 163

2.3. Características. 165
2.3.1. Derecho Innato. 165
2.3.2. Derecho vitalicio e inherente. 166
2.3.3. Derecho Esencial. 166
2.3.4. Necesario. 167
2.3.5. De objeto interior. 168
2.3.6. Temporalmente disponible. 168
2.3.7. Extrapatrimonial. 168
2.3.8. Absoluto. 169
2.3.9. Autónomo. 169
2.3.10. Derecho privado. 170
3. Inviolabilidad del domicilio. 171
3.1. Concepto de domicilio. 173
3.2. Excepciones. 175
4. Secreto de las comunicaciones. 183
4.1. Contenido y ámbito de protección. 189
4.2. Excepciones. 191
5. Origen de la protección de Datos Personales. 199
TERCERA PARTE. Derechos relacionados con las tecnologías Información y Comunicación. 216
CAPÍTULO IV. Situación jurídica de las Tecnologías de Información y Comunicación. 218
1. Consideraciones preliminares. 219
2. Concepto de tecnologías de información y comunicación y características principales. 222
2.1. Inmaterialidad (Posibilidad de digitalización). 225
2.2. Instantaneidad. 226
2.3. Aplicaciones Multimedia. 226
3. Vulnerabilidad de la intimidad en Internet. 228
4. Generalidades sobre Internet. 236
5. ¿Es Internet un Derecho Fundamental? 245
6. Intimidad en Internet. 255
6.1. Cookies HTTP. 256
6.1.1. Según la entidad que las gestione: 261
6.1.2. Según el plazo de tiempo que permanecen activadas: 261
6.1.3. Según su finalidad: 262
6.2. Proveedores de Internet ISP. 265
6.3. Información biométrica e imágenes. 267
6.4. Motores de búsqueda. 272
6.5. Redes sociales. 277
6.5.1. Clasificación de las redes sociales. 279
6.5.2. Intimidad en las redes sociales. 282
6.6. Big Data y la Revolución Industrial 4.0. 287
6.7. Delitos informáticos que protegen la intimidad. 292

CAPÍTULO V. Nuevas dimensiones de la protección de los datos de carácter personal. 308

1. Consideraciones preliminares. 309
2. Derecho fundamental a la protección de datos personales. 315
   2.1. Concepto de autodeterminación informativa o libertad informática. 325
   2.2. Nuevos conceptos y retos en materia de protección de datos personales e intimidad. 330
      2.2.1. La intimidad cognitiva. 330
      2.2.2. La privacidad en el diseño o privacidad desde el diseño (PdD). 333
      2.2.3. La privacidad por defecto (PpD). 340
      2.2.4. Internet de las cosas (IoT). 342
      2.2.5. Falta de control y asimetría de la información. 347
      2.2.6. Calidad del consentimiento del usuario. 348
      2.2.7. Patrones y perfiles de la información relacionados con los hábitos y costumbres de las personas. 350
      2.2.8. La privacidad frente al uso de aviones no tripulados (*drones*). 350
   2.3. Principios de la autodeterminación informativa en la LOPD. 358
3. Derechos de acceso, rectificación, cancelación, oposición y olvido o supresión. 362
   3.1. En los Estados Unidos de América. 362
   3.2. En Europa y España. 367
      3.2.1. Derecho de acceso a los datos personales. 367
      3.2.2. Derechos de rectificación, cancelación, oposición y olvido o supresión. 369
   3.3. En Costa Rica. 377
      3.3.1. Derecho de acceso a los datos personales. 377
      3.3.2. Derechos rectificación, cancelación, oposición y olvido o supresión. 379
4. Excepciones al derecho de protección de datos. 389
   4.1. En los Estados Unidos de América. 391
   4.2. En Europa y España. 393
   4.3. En Costa Rica. 401
5. Derecho al olvido en Internet. 404
   5.1. Breve exposición del caso Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. 407
      5.1.1. Litigio principal. 407
      5.1.2. Planteamiento de la Consulta de prejudicialidad. 408
      5.1.3. Respuesta a la consulta de prejudicialidad. 410
      5.1.4. La parte dispositiva. 412
   5.2. Efectividad del derecho al olvido en Internet y el *efecto Streisand*. 414

CUARTA PARTE. La vigilancia masiva y conclusiones finales. 421

CAPÍTULO VI. Vigilancia masiva de los gobiernos. 423

1. Consideraciones preliminares. 424
2. Historia y origen de la vigilancia global 427
   2.1. Breve recuento histórico de los sistemas de inteligencia y vigilancia antes de los ataques del 9/11. 427
   2.2. Sistemas de vigilancia electrónica. 434

2.3. Cooperación internacional y comercial en la vigilancia masiva. 441
2.4. Agencias de inteligencia de los EE.UU. 446
2.4.1. *Program Managers* (Directores de Programas). 447
2.4.2. Departmental (departamentos gubernamentales). 452
2.4.3. Services (servicios de inteligencia militar). 454
3. Marco jurídico de la vigilancia masiva. 457
3.1. ¿Constitucionalidad y legalidad de la vigilancia masiva de los EE.UU.? 457
3.2. Reacciones y propuestas internacionales ante la vigilancia masiva. 465
3.3. Normativa internacional de Derechos Humanos y la vigilancia masiva. 470
4. Después de las revelaciones de Snowden. 485
4.1. The USA Freedom Act (La Ley de Libertad de los EE.UU.). 485
4.2. Sentencia del Tribunal de Justicia Europeo del 6 de octubre de 2015. 494
4.3. Hacia una nueva forma de protección de la privacidad. 507
CAPÍTULO VII. Conclusiones generales. 532
BIBLIOGRAFÍA. 546
1. Libros y artículos. 546
2. Normativa. 579
2.1. Tratados, Convenios Internacionales y normativa europea. 579
2.2. Constituciones. 580
2.2.1. Nacionales y Federales. 580
2.2.2. Estatales. 581
2.3. Leyes. 581
2.4. Otros instrumentos legales. 586
3. Jurisprudencia. 587
3.1. Resoluciones del Parlamento Europeo. 587
3.2. Corte Europea de Derechos Humanos. 587
3.3. Tribunal de Justicia de la Unión Europea. 588
3.4. Corte Interamericana de Derechos Humanos. 589
3.5. Corte Suprema de los Estados Unidos de América y Cortes Supremas de los Estados. 589
3.6. Tribunal Constitucional de España. 590
3.7. Sala Constitucional de Costa Rica. 591
3.8. Consejo Constitucional de Francia. 592
3.9. Jurisprudencia administrativa. 593
4. Webgrafía. 594

TABLA DE ABREVIATURAS

art., arts.	artículo, artículos
ATC	Auto Tribunal Constitucional
BOE	Boletín Oficial del Estado
CE	Constitución española de 1978
comp.	compilador
coord., coords.	coordinador, coordinadores
dir.	Director
EE.UU.	Estados Unidos de América
DLE	Diccionario de la lengua española
ed., eds.	edición/ editor, editores
inc.	inciso
introd.	introducción
LO	ley orgánica
num.	numeral
No.	número
STC	sentencia Tribunal Constitucional Español
SSC	sentencia Sala Constitucional Costa Rica
t.	tomo
TC	tecnologías de comunicación
TJUE	Tribunal de Justicia Europeo
TI	tecnologías de información
TIC	tecnologías de información y comunicación
trad./ trads.	traductor/ traductores
UE	Unión Europea
vol.	volumen

PRIMERA PARTE. CONTEXTUALIZACIÓN DEL ESTUDIO.

CAPÍTULO I. INTRODUCCIÓN, JUSTIFICACIÓN Y METODOLOGÍA.

"Con toda la atención puesta en los aspectos legales de la privacidad y el impacto sobre el comercio mundial, ha habido poca discusión de por qué uno quiere privacidad y por qué es intrínsecamente importante para uno como individuo".[1]

[1] Adam Joinson, profesor de cambio conductual en la Universidad del Oeste de Inglaterra en Bristol.

1. ABSTRACT.

The following research is a legal study of mass surveillance, the repercussions on privacy rights, secrecy of communications and the protection of individuals with regard to the processing of their personal data.

Initially, we will review the historical origins of the supposed violated rights and the historical evolution of these rights with respect to the growing use and updating of information and communication technologies. Thusly, we will formulate an analysis of the doctrine, legal provisions and case law of privacy rights.

We will set forth the legal challenges faced by the systems pursuing the protection of the fundamental rights and identify some of the issues related to the protection of privacy rights in a contemporary society. Moreover, we will address the matter of mass surveillance as a tool used by technologically advanced governments.

Privacy rights have been considerably impacted by the constant use and globalization of technologies, which have resulted in a necessary adaptation and evolution of these rights in order to continue with the enforcement and defense of the individual rights. The advent of the Internet poses a challenge to the law enforcement agents, which in turn has prompted a movement to propose a legal framework in order to regulate certain activities within virtual environments.

Governments have also benefited from the use of these technologies by using them to generate a significant improvement in addressing their own objectives. However, governments have also taken advantage of other technologies, such as mass surveillance, in efforts to prevent terrorism and other social problems, leading to a negative impact in the privacy and intimacy rights of individuals.

It would appear as though the actions taken by some intelligence agencies have been developed based on a questionable legislation adopted due to the urgency and need to combat terrorism. Thus, these actions resulted in the availability

to access private communications and documents of individuals with the intention to protect the security of their nations. Control and invasion of democratic states in the activities of citizens have been highly questioned which has led to the point of considering that it is a proper model of a totalitarian state, monitoring the activities of all citizens.

Finally, the consequences of this government intrusion will be analyzed to determine whether a balance between the internal security of nations and the free exercise and respect of citizens' rights may be possible.

2. INTRODUCCIÓN.

Los avances de las tecnologías, en los últimos años, han transformado a los seres humanos en muchos sentidos y han permitido un progreso sin precedentes en la historia de la humanidad. La sociedad contemporánea depende en muchos aspectos de las facilidades ofrecidas por las nuevas Tecnologías de Información y Comunicación. La interconectividad y el costo de los dispositivos son algunos de los factores que han generado el acceso a la mayor parte de la población mundial, a una vastísima y variada cantidad de información, acortando los límites espaciales y temporales. Uno de los grandes inventos en este campo es la red Internet, que sin duda ha permitido y facilitado importantes cambios políticos, económicos y sociales.

Junto a las considerables ventajas que representan estas nuevas tecnologías, también han aparecido nuevos problemas y desafíos que causan preocupación en la población. Internet ha actuado como un potenciador de las conductas de las personas con un efecto multiplicador. De esta manera, los derechos y libertades fundamentales se han visto afectados de forma positiva y negativa.

Uno de los derechos más afectados por el uso de las tecnologías de información y comunicación ha sido el derecho de intimidad de las personas. Este derecho se ha visto vulnerado por diversas conductas de los gobiernos, las empresas y personas particulares. La presente investigación se propone analizar una de estas conductas, particularmente la vigilancia masiva, y su contrariedad con los derechos fundamentales de las personas, en especial la afectación que produce a los derechos de intimidad, el secreto a las comunicaciones y la protección de los datos personales.

El derecho de intimidad ha sido reconocido como tal desde el siglo XIX, sin embargo, como valor, tiene antecedentes muy antiguos. Pareciera que la sociedad contemporánea prefiere la seguridad ante el derecho de intimidad, la cuestión es si estos derechos son irreconciliables y si de verdad existe la necesidad de elegir entre

ellos, potenciando uno frente al otro o si, por el contrario, podría existir un balance que permita la seguridad de las personas y se respete su derecho a la intimidad.

Si bien se reconoce el derecho de intimidad como uno de los derechos de la personalidad, lo cierto es que, desde su origen o reconocimiento como parte de los derechos humanos, ha sido necesaria la constante adaptación o evolución para continuar con la vigencia y la defensa de los derechos de las personas, sobre todo teniendo en consideración los avances de las nuevas tecnologías y la capacidad de estas para la potenciar la interacción entre las personas de una sociedad.

La aparición de Internet ha sido causante de que, desde el punto de vista jurídico, sea necesario replantearse la tutela de los derechos fundamentales y readaptarlos a las necesidades de la sociedad contemporánea.

Los gobiernos también han incursionado en la utilización de nuevas y avanzadas tecnologías para cumplir sus objetivos y con ello también se han enfrentado a retos, no solo en la parte instrumental, sino también en la fundamentación propia de sus bases constitucionales y democráticas, readaptándose a estos nuevos retos que son propios de una sociedad tecnológica.

El contenido de los datos o informaciones que se presentan como públicos y privados, se encuentran en constantes procesos de reconciliación y adaptación. Estos procesos, cada vez más agudos, tratan de delimitar, a través de la actividad administrativa y jurisdiccional, los límites de las informaciones y datos a los cuales pueden tener acceso las personas. De una parte, se presenta el derecho al acceso a la información pública, que se traduce en un principio o regla general y como excepción se presenta entonces, la otra parte, que protege el acceso a la información que está reservada a las personas por tratarse de asuntos que son parte de su vida privada.

Constantes intromisiones en la vida privada de las personas son detectadas por parte de las autoridades, que tratan de aplacar de alguna manera las formas ilícitas mediante las cuales se apropian de sus datos, con graves afectaciones a sus

derechos de intimidad, protección de datos personales y secreto a las comunicaciones.

Debe advertirse que tanto las empresas como los gobiernos están interesados en obtener información actualizada sobre las personas, lo cual es entendible, pues con esos datos y las capacidades actuales de los programas informáticos, pueden ser capaces de pronosticar, en muy poco tiempo y a menor costo, las tendencias económicas, políticas y sociales de todo un país o advertir algunas conductas individuales y concretas, pero, en todo caso, con groseras afectaciones de derechos que han sido reconocidos a las personas en la categoría de derechos humanos.

La vigilancia masiva nace como respuesta a los ataques y peligros contra la seguridad nacional, con la utilización de tecnologías que permiten a los gobiernos escuchar las llamadas telefónicas, escanear las redes de datos, leer correos electrónicos y mensajes de texto, seguimiento de personas, incluso cambiar el contenido de los mensajes. Todo ello es factible a través de la utilización de sofisticados equipos electrónicos y programas de computadoras (*software*).

La justificación de la vigilancia masiva, como se indicó, se presenta como la mejor solución para combatir el terrorismo, evitar los conflictos sociales y proteger la seguridad nacional de los Estados a nivel internacional. La crítica principal a estos sistemas radica en el hecho de que la vigilancia no discrimina a los sujetos investigados, recae en una gran parte de la población civil que no está involucrada en actividades ilícitas, lo que afecta, consecuentemente, los derechos fundamentales, civiles y políticos de la población en general.

Revelaciones recientes exponen a la luz las técnicas y capacidades de los gobiernos para vigilar a la población y hacen parecer que hoy se vive en el *distópico* mundo creado por Eric Arthur Blair, conocido como George Orwell, en su novela

política “Nineteen Eighty-Four”[2] en la cual se da a conocer el concepto de “Gran Hermano” desde su publicación en 1949. Algunos paralelismos, de la actual era digital y la novela de Orwell han sido expuestos por los analistas[3], quienes relacionan la manipulación de la información, las prácticas de la vigilancia masiva y la represión política y social, como elementos análogos de la sociedad contemporánea.

El concepto orwelliano del “*Gran Hermano*” pareciera se ajusta a las posibilidades tecnológicas de la época actual, que posibilitan a los gobiernos el espionaje en dimensiones que antes solo eran posibles en las novelas de ciencia-ficción. Una de las cuestiones principales a determinar en esta investigación es si es necesaria la vigilancia masiva indiscriminada de las personas, sustentada en razones de seguridad nacional o si, por el contrario, se trata de un exceso por parte de las autoridades gubernamentales en los mecanismos empleados por las agencias de inteligencia.

Organismos no gubernamentales han alzado su voz frente a la vigilancia masiva llevada a cabo por los gobiernos. Para ello han recurrido tanto al planteamiento de denuncias ante organismos internacionales de protección de derechos humanos, como a campañas de sensibilización y protesta ante los ultrajes de las agencias de espionaje que han colaborado entre sí, así como con empresas privadas.

Uno de los propósitos fundamentales de la presente investigación es determinar si con el afán de crear sociedades más seguras, es necesario renunciar

---

[2] ORWELL, G., *Nineteen Eighty-Four*, ed. Penguin Books, 2013, [edición para lector digital Kindle].

[3] Edward Snowden indicó que Orwell ya había advertido de los peligros de la vigilancia masiva del gobierno, en un mensaje de Navidad transmitido por televisión para el Reino Unido. WITTE, G., “Snowden says government spying worse than Orwellian” en *The Washington Post*, 25 de diciembre de 2013, [en línea], https://www.washingtonpost.com/world/europe/snowden-says-spying-worse-than-orwellian/2013/12/25/e9c806aa-6d90-11e3-a5d0-6f31cd74f760_story.html

a la intimidad y, de ser así, establecer cuáles podrían ser los límites y las medidas necesarias para protegerse ante los posibles excesos o abusos.

Como forma de abordaje del tema y, a efectos de la investigación que se presenta, se ha estimado necesario abordar algunos antecedentes históricos relevantes, así como señalar los derechos humanos y constitucionales involucrados en el tema de la intimidad y puestos en riesgo con la vigilancia masiva, a fin de determinar conceptos que ubiquen y delimiten la presente investigación. Se propone una contribuir con el estudio de un problema que afecta a millones de personas en el mundo, para determinar sus alcances jurídicos, los riesgos, las vulneraciones y las posibles soluciones ante la afectación de derechos humanos fundamentales, como el derecho de intimidad, la protección de datos personales y la inviolabilidad de las comunicaciones.

La investigación inicia con la delimitación de los conceptos de intimidad y privacidad, para lo cual se realiza un estudio histórico de estos términos como valores en la sociedad. Resulta necesario establecer y delimitar los alcances jurídicos de cada uno de esos conceptos, pues de forma regular suelen utilizarse sin hacerse ninguna distinción. En la práctica jurídica es frecuente el uso de estos términos como sinónimos, suelen confundirse porque aparentan cubrir los mismos aspectos, pero como se expone en este trabajo, tienen diferente significado, cubren diferentes aspectos y su distinción es importante para brindarles la necesaria protección, motivo por el cual resulta indispensable ahondar no solo en la delimitación sino también en el origen de los términos, con el fin de determinar el alcance y el ámbito de aplicación de cada uno de ello, tal y como se expondrá.

Los orígenes del derecho a la intimidad son reconocidos en el derecho anglosajón. En un principio, se concebía como el derecho a estar solo (*the right to be let alone*), otorgándosele un contenido negativo, oponible por los titulares frente al resto de las personas. Desde entonces hasta la actualidad el derecho de intimidad ha evolucionado considerablemente, pasando a convertirse en un derecho de contenido positivo, por medio del cual las personas tienen la facultad de elegir

cuanto de su vida privada desean exponer ante otras personas, sin embargo, el avance de las nuevas tecnologías ha sido tal que ha hecho vulnerable este derecho, requiriendo que se amplíen los mecanismos jurídicos para su protección.

Asimismo, en este trabajo se expone el largo recorrido y el amplio desarrollo que ha tenido este derecho para evidenciar los problemas que se presentan en la sociedad tecnológica contemporánea a través de un repaso de las teorías, la normativa, las características y los derechos que se consideran se han desprendido de este, tales como, el derecho de imagen, el honor, la inviolabilidad del domicilio, el secreto a las comunicaciones y, de forma más reciente, la protección de los datos personales.

Actualmente se reconoce el derecho a la protección de los datos personales como un derecho autónomo y derivado del derecho a la intimidad. Se trata de un derecho relativamente reciente, el cual ha evolucionado para proteger los datos de las personas ante el constante avance de las tecnologías, las cuales tienen la capacidad de convertir casi todo lo que nos rodea en datos. La tutela de este derecho ha generado la creación de agencias de protección de datos, las que, mediante procedimientos administrativos, se han convertido en la primera línea de defensa y protección de los datos de las personas, al menos en los lugares donde han funcionado con cierta eficacia. Estos mecanismos de defensa por ser más recientes, expeditos, menos onerosos o gratuitos, tienden a ser sumamente efectivos cuando son utilizados con responsabilidad, conforme se expondrá y justificará más delante.

Por último, en el presente trabajo se analizan los aspectos legales y jurisprudenciales de la vigilancia masiva que han venido utilizando algunos gobiernos con la colaboración de algunas empresas privadas. Se tendrán en cuenta para el análisis, las reacciones de diversos sectores de la sociedad, organizaciones no gubernamentales y Tribunales Internacionales.

En síntesis, el trabajo pretende poner en evidencia cómo los programas de vigilancia masiva utilizados por algunos gobiernos, con el auxilio de algunas empresas privadas, afectan la vida privada de las personas y lesionan derechos fundamentales, como el derecho de intimidad, la protección de datos personales y la inviolabilidad de las comunicaciones, señalándose hasta dónde el ordenamiento jurídico y los mecanismos de tutela jurídica han funcionado para brindar protección.

2.1. Justificación.

Actualmente la intimidad en Internet es objeto de innumerables estudios, discusiones, análisis y noticias. Todas estas discusiones generan curiosidad entre los más diversos sectores de la sociedad. Tal vez uno de los casos más emblemáticos y fuente de nuevas y vigentes discusiones, sea el de Edward J. Snowden, ex analista de la Agencia de Seguridad Nacional (NSA) quien reveló información sobre programas de vigilancia masiva (PRISM) por parte del Gobierno de los Estados Unidos de América (EE.UU.). A este se suman otros casos, producto del almacenamiento y venta de datos por parte de grandes empresas relacionadas con servicios en la red o indiscreciones obtenidas en los contenedores de datos en la nube o *cloud computing,* como el caso de los desnudos publicados de la actriz de Hollywood Jennifer Lawrence[4] en el mes de setiembre de 2014.

El uso de la tecnología, ya sea sin los cuidados pertinentes o mediante actuaciones dolosas de otros, puede generar daños en la privacidad e intimidad de las personas de muy difícil o imposible reparación. Cada vez más las personas toman conciencia de lo perjudicial que puede resultar el manejo de sus datos en línea, dado que pueden ver afectada su intimidad por la intervención de terceras personas. Por ello, desde diversos sectores o áreas del conocimiento se proponen alternativas para minimizar esas afectaciones al derecho de intimidad de las personas.

El derecho a la intimidad se ha consagrado como la base jurídica del derecho a la protección de los datos personales. Sin embargo, como se expone en el trabajo,

[4] Según varios medios estadounidenses, los piratas accedieron a bancos de datos del sistema de almacenamiento en línea *iCloud* de la empresa Apple, aunque no se descartan las intervenciones de otros sitios de almacenamiento en la *nube*. Al efecto se puede consultar sobre la noticia en: http://www.nacion.com/ocio/farandula/Apple-FBI-investigan-estrellas-Hollywood_0_1436656403.html

muchos autores coinciden al señalar estos derechos como insuficientes frente al vertiginoso crecimiento de las nuevas tecnologías de información y comunicación.

Se reconoce el derecho de intimidad como un derecho humano esencial en las sociedades democráticas. Es esencial a la dignidad humana y refuerza otros derechos, como la libertad de expresión y de información, así como la libertad de asociación.

La protección jurídica de la intimidad, aunque muy importante, pareciera no ser una completa solución para la protección de los datos e intimidad de las personas, por lo menos se habla de los datos compartidos en Internet. Los límites de jurisdicción territorial, la falta de personalidad, la gran capacidad de almacenamiento, el constante avance y refinamiento de tecnologías que facilitan la vigilancia y el interés económico, podrían ser algunas de las causas que impiden una adecuada protección.

La información de los usuarios de Internet se ha convertido en la mercancía con la que algunas empresas se hacen multimillonarias. Así lo afirmó Federico Zannier, ex empleado de Microsoft Xbox, en un comunicado puesto en Kickstarter (un portal de micromecenazgo o *crowdfunding*) en el cual, a modo de reivindicación, señaló que en las políticas de privacidad de las páginas que suele visitar, ha encontrado frases como esta: *"usted otorga una licencia mundial no exclusiva y libre de derechos para usar, transmitir y distribuir cualquier contenido en todos los medios de distribución (conocidos o por desarrollar)"*[5]. Es decir, al aceptar esas condiciones

[5] MUÑOS, F., "¿Cuánto cuesta tu historia en Internet?", en *ABC.es,* 15 septiembre 2014, [en línea], Http://www.abc.es/tecnologia/redes/20140907/abci-cuanto-vale-usuario-internet-201409051544.html

se permite que se usen los datos personales según lo decida la empresa que los procesa.

La empresa Syncapse ha realizado un estudio titulado *"El valor de un Fan en Facebook"*, donde se ha analizado el impacto del consumidor en las redes sociales. Syncapse ha señalado que el valor medio de un seguidor de una Fan Page de una marca es de $174 dólares según datos del año 2010; este valor, a la fecha, se ha incrementado en un 28%[6].

El desarrollo de estas tecnologías tiene elementos que han potenciado su alcance en la sociedad, entre ellas: la interconexión[7] y la convergencia[8]. En un inicio, las tecnologías informáticas tenían la capacidad del almacenamiento masivo de información a lo que luego se sumaron las capacidades de interconexión y convergencia, lo que las hace propicias para vulnerar algunos derechos, entre ellos los personales.[9]

---

[6] Para realizar este estudio, Syncapse trabajó con la firma de investigación Hotspex con la que recogió información de más de 2,000 especialistas de marcas estadounidenses entre enero y febrero de 2015. Para obtener estos datos se compararon los datos de los fanáticos en Facebook, el gasto correspondiente, la lealtad a la marca, la forma en que recomiendan la marca y otras variables. En un informe publicado en 2010 demostraron que los seguidores en Facebook son un segmento extremadamente valioso en la audiencia en internet, y un segmento valioso de los consumidores [en línea], http://www.syncapse.com/value-of-a-facebook-fan-2013/#.VCzm0Pl5N8G

[7] Esta es la posibilidad que tienen los aparatos electrónicos, de intercambiar datos, permite el acceso a una serie de servicios y prestaciones adicionales.

[8] Por su parte, la convergencia se define como la interconexión de las tecnologías de la computación e información, *i. e.* es la mezcla de las tecnologías *e. g.* los teléfonos móviles que posibilitan la televisión, acceso a internet, cámara fotográfica, etc.

[9] *Vid.* GARCÍA MEXIA, quien expone que las nuevas tecnologías, por su naturaleza de unión, se abren al exterior sin límites aparentes, lo que plantea dudas sobre la protección de los derechos básicos de los individuos. *"Las nuevas tecnologías ya no son, solamente, una herramienta útil en las funciones rutinarias de gestión y control económico de la empresa en su faceta interior; las nuevas tecnologías tienen su verdadero interés en la unión -casi por naturaleza- con las telecomunicaciones y su apertura hacia el mundo exterior que, al no tener límites aparentes, plantea serias dudas en*

A pesar de las numerosas noticias sobre afectaciones a la intimidad, que aparecen todos los días en los medios de comunicación, no ha disminuido el uso de estos artefactos y servicios. La mayoría de fuentes que se consultaron, ponen en evidencia el creciente número de usuarios y accesos tecnológicos, así como el aumento de servicios brindados por medio de las nuevas tecnologías.

Desde el punto de vista social, es entendible que las personas no quieran, np deban o no puedan quedar aisladas del mundo electrónico. En muchas investigaciones se habla de la nueva *sociedad de la información o del conocimiento* y varios autores han emitido criterios sobre el relevante impacto en el comportamiento de las personas y el cambio social producido por los avances de la tecnología[10].

Probablemente, el término de *sociedad tecnológica electrónica,* es el que mejor se ajusta a la creciente preeminencia que ha adquirido la tecnología en las diversas áreas de la economía, la sociedad y la cultura. La comunicación tecnológica electrónica se está convirtiendo cada vez más en una característica importante de nuestra sociedad, a tal grado que algunos autores coinciden en que se ha generado un nuevo entorno social. Con esta tecnología se crea un nuevo tipo de economía y de sociedad, transformando las relaciones entre los seres humanos

---

cuanto al respeto de los derechos básicos de los individuos y su estructuración en una diferente organización social, que permita no poner puertas al campo, con el paralelo respeto a los derechos de la persona y su desarrollo en libertad dentro de la convivencia; con una regulación jurídica -junto a unos presupuestos éticos-, de los comportamientos básicos en el respeto y libertad que definen y distinguen al hombre". GARCÍA MEXÍA, P. (dir.), *Principios de Derecho de Internet,* Tirant lo Blanch, Valencia, 2ª ed., 2005, p. 27. *v. et*. HERREA BRAVO, R., "Ciberespacio, sociedad y derecho", en RICO CARRILLO, M. (coord.), *Derecho de las nuevas tecnologías,* Ediciones la Rocca, Buenos Aires, 2007, pp. 35-37.

[10] JOINSON, A. y PIWEK, L., "Technology and Behaviour Change: For good and evil", *Social impact of technology*, STI Press, New York, Agosto 2013, [en línea], http://www.joinson.com/home/pubs/joinson_piwek.pdf

al abrir nuevos cauces para experimentar la realidad, que posibilitan una nueva dimensión, la dimensión virtual.

Una de las características de este nuevo modelo de organización es el acercamiento de las personas a la información, basándose en las enormes posibilidades comunicativas derivadas de la aplicación de las tecnologías al almacenamiento, procesamiento y distribución de la información.

En los instrumentos internacionales[11] de derechos humanos, así como en la mayoría de legislaciones locales, se protegen los derechos de las personas relacionados con la privacidad, intimidad y el resguardo de sus datos personales. Estos derechos pueden verse disminuidos cuando aparecen problemas graves que afectan a la sociedad, siendo el principal problema el de seguridad. Ciertamente, los avances en la tecnología han permeado muchas áreas y son aprovechados por los gobiernos y empresas privadas para solucionar algunos problemas que también afectan a la sociedad o, simplemente, para mejorar ciertas actividades de la vida cotidiana. Lo grave son los usos arbitrarios y groseros de esas tecnologías contra las personas o bien la amplia discrecionalidad con la cual han operado ante la falta de una adecuada regulación.

---

[11] Convención Americana sobre Derechos Humanos (Pacto de San José), suscrita en Costa Rica el 7 del al 22 de noviembre de 1969, dispone en el artículo 11 que: "*1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. 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. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".* Declaración Universal de Derechos Humanos, Artículo 12, Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares, Artículo 14, Convención sobre los Derechos del Niño de Naciones Unidas, Artículo 16, Pacto Internacional de Derechos Civiles y Políticos Artículo 17; convenciones regionales incluido Artículo 10 del Capítulo Africano Carta sobre los Derechos y el Bienestar del Niño, Artículo 4 de los principios de la Unión Africana sobre la Libertad de Expresión, Artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre, Artículo 21 de la Declaración Derechos Humanos de la ASEAN, Artículo 21 de la Carta Árabe de Derechos Humanos, y Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; Principios de Johannesburgo sobre la Seguridad Nacional, Expresión y Acceso a la Información, Principios de Camden para la Libertad de Expresión y la Igualdad Libre.

Uno de los sistemas que ha logrado una interconexión global ha sido la red denominada Internet, la cual ha alcanzado una penetración en ámbito mundial y ha sido generadora de una serie de cambios en la sociedad. Este sistema de redes es la causa principal de la interconexión entre los aparatos electrónicos, aunque como se verá más adelante, no es el único sistema o tecnología que ha permitido el grado de interconexión que tienen actualmente los dispositivos electrónicos.

Se debe tener presente que el desarrollo social y moral del ser humano nunca ha sido contrario al desarrollo de las realidades técnico científicas. Estas realidades influyen en el cambio social y producen nuevos valores, nuevos paradigmas éticos y, en definitiva, el advenimiento de nuevas formas de organización social.

Plantear la regulación sobre el uso y alcances de las nuevas tecnologías de la información y comunicación no es un tema fácil, pues su repercusión ha sido colosal. En el desarrollo de esta investigación se analizará cómo, en razón de estas nuevas tecnologías, se han creado un gran número de regulaciones y hasta el reconocimiento de derechos que se consideran “nuevos o emergentes” o bien “fundamentales”.

Las estructuras normativas surgidas en la modernidad y en la etapa de la codificación, no han podido sustraerse a los efectos de la creciente aplicación de tecnologías, característica de la *sociedad tecnológica electrónica*.

Todos estos avances tecnológicos, por su carácter radicalmente nuevo, crean una nueva problemática que supone un reto para el jurista. La realidad, cada vez más compleja y cambiante, exige no sólo la adaptación de conceptos y teorías jurídicas al nuevo medio, sino que, en muchos casos, impone la creación de otros nuevos. Se afirma que la naturaleza de los cambios que se están produciendo es

tal que somete a una dura prueba no sólo a conceptos y nociones tradicionales, sino también a aspectos estructurales del Derecho. [12]

La informática ha reducido las dimensiones del mundo actual por medio de una red de comunicación y almacenamiento de datos. Esto se ha convertido en un valor de mercado y por ello la frase -ya clásica- de que *la información es poder*, ha dejado de ser un mero eslogan para pasar a ser una realidad incuestionable[13].

Toda revolución tecnológica lleva consigo una reorganización económica, política y social. Las posibilidades de almacenamiento, tratamiento y control de la información que ofrece la Informática pueden convertirla en un instrumento de presión y control social que amenaza la libertad del individuo. Este peligro se hace más palpable en el sector público, el cual concentra gran cantidad de información[14].

---

[12] PÉREZ LUÑO señala que *"En las nuevas sociedades informatizadas, el poder ya no reposa en el ejercicio de la fuerza física, sino sobre el uso de informaciones que permitan controlar las conductas de los ciudadanos".* PÉREZ LUÑO, A. E., "Los Derechos Humanos en la Sociedad Tecnológica". Madrid, Cuadernos y Debate, en vol. *Libertad Informática y Protección de Datos Personales*, Centro de Estudios Constitucionales, 1999, p. 67.

[13] La revelación del programa PRISM, que permite a EE.UU. espiar a los usuarios de Internet, provocó un gran escándalo mundial, pero en realidad los datos personales compartidos en la Red global ya se convirtieron hace años en una "mercancía", según informa el suplemento económico del periódico francés 'Le Figaro', que analiza la 'lista de precios' de esta información. Gigantes informáticos como Facebook, Google, Amazon, Apple y Microsoft, entre otros, disponen de enormes bases de datos sobre los usuarios y las venden a las compañías para una colocación más acertada de anuncios publicitarios de sus productos o servicios. Este mercado ya se valora en unos 100.000 millones de dólares, pero llegará a su máximo desarrollo en los próximos diez años, según un estudio de la compañía consultora Roland Berger, citado por 'Le Figaro'. *RT ¡sepa más!.* 23 de julio de 2013, [en línea], http://actualidad.rt.com/economia/view/100873-marketing-publicidad-online-datos-personales; sobre el programa secreto PRISM ver *infra* Cap. VI. 2.2.

Se estima que existen entre 3500 y 4000 empresas que se dedican a la intermediación de datos electrónicos, a las cuales se les conoce como corredores de datos *(Data Brokers).*

[14] GOMEZ NAVAJAS, J., *La protección de datos personales*, Editorial Aranzadi, Navarra, 2005, p. 33.

Los poderes públicos realizan, en ocasiones, intromisiones en la esfera privada y la dignidad personal que afectan, directamente, la participación democrática del ciudadano, ya que la concentración de información y su tratamiento en centros de poder puede favorecer el abuso por parte de estos; tal acción puede impedir el control y el acceso de las informaciones por parte del ciudadano, lo que hace indispensable la protección del derecho a la intimidad del individuo frente al celo del Estado por defender sus intereses generales.

Quizá sea suficiente, además de lo ya indicado, para terminar de convencerse sobre las violaciones a la intimidad en Internet, ver un documental realizado por Cullen Hoback, llamado *"Terms and conditions may apply"* (aplican términos y condiciones)[15], para enterarse de la arbitrariedad de las políticas de privacidad y aplicaciones que se utilizan en los sitios web. Basta con que se navegue en la red para dejar, de modo no consciente, una serie de datos que son utilizados por las empresas bajo el *supuesto consentimiento* en un contrato de letra pequeña, en el que se autoriza la utilización de los datos que se suministran; además, en algunos supuestos *se consiente* que las cláusulas de privacidad puedan ser modificadas de forma unilateral por parte de la empresa, sin necesidad de notificación alguna.

Existen empresas que se dedican, únicamente, a recopilar y analizar datos que alimentan una industria casi secreta; estas no acceden a datos directamente, sino que los crean. Los corredores de datos (*data brokers*), los analizan para venderlos a otras compañías, es decir, funcionan como mediadores en el rentable mercado de datos de consumidores. En un informe del Senado de los EE.UU. se

[15] CULLEN HOBACK, Documental filmográfico, *Terms and conditions may apply***,** 2013 [en línea], http://www.rocofilms.com/film.php?code=TACM

denunciaron las actividades de nueve[16] de estas empresas y se confirmó que controlaban los datos de más de 700 millones de personas[17]. La información que tienen estas empresas es de carácter personal, íntimo y se refiere tanto a los estados financieros como a datos relacionados con la salud de las personas[18].

Ahora bien, una noticia que ha generado alarmas respecto de la intimidad de los datos es la reciente compra, por parte de la empresa Google, de la compañía Dropcam, dedicada a vigilar hogares[19]. Se trata de una empresa creada en el año 2009, que ofrece cámaras y servicios de vigilancia para ser colocadas a lo interno de los hogares.

Evidentemente, la preocupación de los usuarios se hizo manifestar, al pensar que esta empresa, que ya controla muchos de los datos de las personas, pueda obtener nueva información de ellas, pues ahora es fácil obtener sus datos: con un reloj digital monitorean la salud, se obtienen datos de consumo en los termostatos de las casas, se obtienen preferencias de los usuarios que tienen televisores con el adaptador Chromcast y puede inferirse los destinos y frecuencias de los usuarios de los autos o coches. Junto a la citada compra, está por definirse próximamente la adquisición de Skybox, empresa fabricante de satélites.

---

[16] Las empresas denunciadas son Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, Recorded Future.

[17] Senado de los Estados Unidos de Norteamérica, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes,* Diciembre de 2013 [en línea], http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577

[18] *Ibíd.,* p. 12.

[19] JIMÉNEZ CANO, R., "Google compra Dropcam, dedicada a vigilar hogares", en *El país,* 21 de junio de 2014, [en línea], http://tecnologia.elpais.com/tecnologia/2014/06/21/actualidad/1403328618_189486.html

Cuando se activan los servicios de Google en el teléfono móvil, inevitablemente se integran los correos, el GPS (servicio de Google Maps), servicios de almacenamiento de datos (Google Drive), la tienda de aplicaciones (Google Play), servicios de lectura (Google Reader) y, por supuesto, el buscador en Internet (Google Search), entre los muchos servicios que ofrece tal empresa. El hecho de poder conectar todos los datos generados por estas aplicaciones permite conocer, casi de modo absoluto, cualquier dato sobre un usuario, incluyendo los más íntimos, ya sea porque se compartieron esos datos o porque se infieren de otros suministrados[20].

[20] Se pude ver una lista completa de los servicios ofrecidos por la empresa Google [en línea]: http://www.google.com/intl/es-419/about/products/

2.2. Planteamiento de la Investigación.

En junio de 2013, un ex agente de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos (EE.UU.), Edward Snowden, revela y denuncia la existencia y el uso de programas de vigilancia masiva implementados por parte de este gobierno con el supuesto propósito de detectar información relacionada con el terrorismo y contraespionaje y agregó que esa vigilancia se extendió a más de 193 países del mundo[21].

Según las denuncias de Snowden[22], el gobierno de los EE.UU., con la colaboración de algunas empresas de TI y otros gobiernos, han utilizado programas informáticos para vigilar la actividad de todas las personas en línea. Entre los documentos filtrados por el ex agente, se encuentra información de millones de usuarios de Internet y telefonía, los cuales fueron obtenidos derivándolos de llamadas, correos electrónicos, videos, foros, fotos, transferencia de archivos y otras acciones comunes en las redes sociales y servicios en la web, que habían realizado los propios usuarios.

En principio tal ventaja del gobierno de los EE.UU. se dio luego de los ataques del grupo terrorista *Al Qaeda* contra el *World Trade Center* y el Pentágono,

---

[21] En una representación de las capacidades de vigilancia de la agencia, se reveló que ésta recogía 5.000 millones de registros de ubicación de teléfonos móviles al día y 42.000 millones de registros de Internet —incluidos correos electrónicos e historiales de navegación— al mes, Amnistía Internacional, [en línea], https://www.es.amnesty.org/noticias/noticias/articulo/una-encuesta-de-amnistia-internacional-revela-la-oposicion-global-a-la-vigilancia-masiva-de-estado/

[22] Las fuentes utilizadas para exponer el caso de las revelaciones de Edward Snowden son tomadas, principalmente de los periódicos *The Guardian y The Washington Post,* pues a través de estos medios se dieron a conocer las importantes revelaciones, las que también han sido confirmadas en la publicación del Periodista y Abogado Gleen Greenwald, quien entrevistó de forma personal a Snowden en Hong Kong, en la obra "*No place to hide"*, Macmillan's, New York, 2014, [versión para lector digital Kindle].

pues la NSA siguió las órdenes del presidente George W. Bush para iniciar la recopilación nacional sin autorización del Congreso y los tribunales, en ese momento.

En las revelaciones que hace Snowden se infiere que, bajo el programa PRIMS, el gobierno de EE.UU. puede obtener los datos de los usuarios de las empresas Google, Microsoft, Yahoo, Apple y otras cinco compañías con sede en los EE.UU.[23]

En la actualidad se discute en el Congreso de los EE.UU. una reforma a la "Ley Patriota", la cual permite la recolección de datos por parte de la NSA. La disputa entre el derecho de Intimidad (*privacy*) y la Seguridad Nacional están sobre el tapete de negociaciones entre los congresistas republicanos y los demócratas.

Estos hechos han generado grandes debates y replanteamientos en muchas disciplinas, entre estas, la jurídica. El asunto es distinguir si se trata de novedades fáctico jurídicas frente a problemas, en apariencia novedosos y complejos o si, por el contrario, se trata de asuntos que en esencia ya habían sido planteados y resueltos con anterioridad[24].

¿Se podrían resolver las tensiones existentes entre, intimidad y seguridad, en una época amenazada por el terrorismo, altamente dominada por la vigilancia estatal y la utilización de TIC's?, si esto fuese posible, ¿cuál sería la forma de

---

[23] GREENWALD, G., *No place to hide, op. cit.,* [versión para lector digital Kindle].

[24] Hace más de 125 años, se planteaba cómo los avances tecnológicos podrían irrumpir en la vida privada de las personas, derecho que se anteponía en aquel momento a la libertad de prensa y expresión. Un clásico jurídico del derecho de intimidad, señalaba entonces a las cámaras fotográficas como un aparato tecnológico capaz de afectar la intimidad de las personas. WARREN S. D., y BRANDEIS, L. D., "The Right to Privacy", en *Harvard Law Review*, 4, 1890, [en línea], http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

resolver estas tensiones?, ¿sería suficiente la autorregulación en Internet, o se necesitan leyes que regulen la actividad de los estados y las empresas? Muchas otras interrogantes de importancia y complejidad, con relación a los derechos de intimidad, protección de datos, libertad de expresión, libertad de comercio y otros derechos fundamentales, se plantean en la actualidad y necesitan ser abordadas.

El tema de protección de la intimidad y la protección de datos personales, en una era digital, empieza a cobrar importancia entre la población[25], sin embargo, pareciera existir en los ciudadanos, una gran confusión entre ambos derechos, de los cuales, si bien reconocen su existencia, desconocen los alcances y la necesidad de la protección.

Da la impresión de que los derechos de intimidad y la protección de datos han sido relegados y tratados frente a la seguridad y vigilancia, como derechos individuales que no tienen relación con la colectividad. Incluso habría que preguntarse hasta dónde los ciudadanos están dispuestos a ceder derechos a cambios de seguridad, hasta qué punto podrían consentir una disminución en sus ámbitos de privacidad frente al combate de la criminalidad, pero el problema más grave es que esas renuncias han sido tácitas o aceptadas con poca conciencia de su magnitud.

Podría ser que se haya sobredimensionado la seguridad frente al derecho de intimidad, sin embargo, una reciente encuesta demuestra que el 71% de las personas entrevistadas rechazaba rotundamente el control de Internet por Estados Unidos, casi dos tercios afirmaban que querían que las empresas de TI (como

---

[25] El *Public Awareness Survey 2008*, realizado por el *Irish Data Proteccion Commissioner,* [en línea], http://www.dataprotection.ie/documents/press/Survey08.pdf muestra como tercera preocupación de la población la intimidad, un 84% de los encuestados lo calificó como un asunto muy importante a tres puntos debajo de la prevención del crimen.

Google, Microsoft y Yahoo!) protegieran sus comunicaciones para impedir el acceso del gobierno[26].

Lo anterior ha motivado a plantear como hipótesis central de este trabajo lo siguiente:

Los programas de vigilancia masiva, utilizados por algunos Estados, con la colaboración de las empresas privadas de Internet, autorizados por una legislación permisiva centrada en la seguridad nacional, vulneran los derechos fundamentales de las personas protegidos en la normativa internacional de Derechos Humanos, tales como el derecho de intimidad, la protección de datos personales, la inviolabilidad de las comunicaciones, afectando con ello el desarrollo de la vida privada de las personas.

Para protegerse frente a posibles demandas de los ciudadanos, las empresas TIC proceden, en forma constante y sistemática, a obtener de ellos su aprobación y consentimiento al momento en que descargan los programas o sus actualizaciones, donde se establecen una gran cantidad de cláusulas que deben ser aceptadas por adhesión, sin posibilidad de negociar o rechazar alguna, bajo pena de no poder utilizar el programa que se desea.

Y resulta que, en el mundo de hoy, no utilizar esos programas informáticos y no estar conectado a Internet implica, prácticamente, el aislamiento total o la imposibilidad de desenvolverse con normalidad en sociedad, de estudiar, de emprender un negocio, de realizar una actividad profesional, de comunicarse con los usuarios y clientes, incluso hasta para realizar programas en las propias instituciones públicas, solo para mencionar algunos ejemplos. La vida laboral, profesional, incluso hasta la familiar y personal no es posible sin el apoyo de los

[26] YouGov Plc, encuestas realizadas entre 4 y 16 de febrero de 2015, [en línea], https://www.es.amnesty.org/dejendeseguirme/encuesta

numerosos programas informáticos de comunicación y sin acceso al Internet, de ahí que se haya constituido en un derecho fundamental para el ser humano, sin el cual resultaría imposible desenvolverse en adelante.

2.3. Alcances y limitaciones.

El objeto de esta investigación se limita al estudio de los efectos jurídicos producidos por la vigilancia masiva realizada por parte de algunos gobiernos con la colaboración de algunas empresas privadas. Se pretenden describir los principales retos que en la actualidad enfrentan las personas al ver lesionados sus derechos fundamentales, ante la utilización de nuevas tecnologías que permiten obtener información sensible y privada sobre ellas.

En la elaboración del planteamiento se han recurrido a diversos tipos de fuentes, entre las que destacan las doctrinales, legales y jurisprudenciales. Tratándose de un problema muy reciente, el abordaje al objeto de estudio se dispuso de forma tal que, desde el Derecho Constitucional, se traten los aspectos principales de los derechos lesionados por esa actividad, principalmente la realizada por parte de los gobiernos.

Al tratarse de una actividad secreta realizada por parte de las agencias de inteligencia de varios países, debe advertirse que alguna información que ha sido revelada, de forma relativamente reciente, aún no ha sido completamente verificada, lo que permite dudar de la veracidad de algunas afirmaciones, y ello se traduce como límite de la investigación impuesto por el problema objeto de estudio. No obstante, se debe señalar que todas las afirmaciones hechas en la presente investigación han sido debidamente respaldadas, citándose la fuente de donde se obtuvo la información y la forma de consultarla. Desde luego, alguna especulación se realiza respecto de algunas actividades secretas realizadas por los gobiernos, pero en todo caso, aquella información que se consideró especulativa fue debidamente indicada.

De otra parte, el objeto principal de la investigación está circunscrito a los Estados Unidos y Europa, por un lado en virtud de que en esas regiones se encuentran los estados que, dado su altísimo nivel de desarrollo, han podido realizar o utilizar en mayor medida las técnicas de vigilancia masiva de datos y, por otro,

que por esa misma circunstancia, en esas regiones es donde, en mayor medida, se ha presentado la discusión sobre la necesidad de proteger la intimidad y ha habido un mayor desarrollo jurídico dirigido a su tutela. Además, en esta investigación se hacen referencias concretas del derecho español y costarricense a efectos de ilustrar, situaciones relacionadas con el tratamiento de estos derechos.

Asimismo, debe señalarse que se utilizaron diversas metodologías y técnicas como herramientas de la investigación con el propósito de lograr un encuadre adecuado del objeto del estudio. Se advierte finalmente que el objeto de estudio de la presente investigación no es exclusivo del Derecho Constitucional, incluso ni de las Ciencias Jurídicas, pues una gran cantidad de las actividades cotidianas de las personas están relacionadas con la utilización de tecnologías de información y comunicación y, en su mayoría, interesan tanto al estudio del Derecho, cuanto a otras ciencias y disciplinas, como la informática, las ciencias de la comunicación, la economía, la sociología, la moral, la religión, la psicología, la antropología, la historia, las ciencias políticas, solo para mencionar algunas. Así como ahora se aborda todo el proceso histórico de la revolución industrial, y su gran influencia en todas las relaciones humanas, así es probable que se llegue a abordar, sin precisar en cuántos años, la era de la revolución digital que se está atravesando, y lo peor, es que ni siquiera se puede saber si apenas está iniciando.

3. METODOLOGÍA Y OBJETIVOS.

3.1. Metodología.

Este trabajo de investigación se circunscribe al estudio de la vigilancia masiva y la afectación de los derechos fundamentales relacionados con la intimidad, tales como el derecho de imagen, el derecho al secreto de las comunicaciones y la protección de los datos de las personas, derechos que se estiman se han desarrollado y han evolucionado para ampliar su protección ante el crecimiento, utilización y globalización de las tecnologías de información y comunicación.

La obtención de fuentes jurídicas doctrinales de un tema tratado de forma interdisciplinaria, supuso un reto al investigador que, con el tiempo, se tradujo en una ventaja pues se vio en la necesidad de ampliar las técnicas y formas investigativas, a efectos de obtener los insumos necesarios para adentrarse en el estudio jurídico de un tema trascendental en el área de los Derechos Humanos y el Derecho Constitucional.

A través de la historia han ocurrido hechos relacionados con la vigilancia indiscriminada y arbitraria, sin embargo, de forma reciente se ha revelado la utilización de un nuevo tipo de vigilancia, la vigilancia electrónica, tema que de reciente data inició un gran debate en la academia y diversos sectores de la sociedad.

Así, se requirió consultar de forma electrónica libros, artículos de revistas, leyes, jurisprudencia, noticias, entre otros, lo cual se localizó en diversas bibliotecas electrónicas tales como Vlex, Dialnet y Ebsco, lo que finalmente permitió realizar un estudio mucho más en el ámbito nacional y de otros países. Otra fuente de consulta y adquisición de libros y artículos físicos y electrónicos fue a través de la compra en línea en Internet. También se tuvo acceso a obras doctrinales, normativa y jurisprudencia ofrecidas en las páginas electrónicas de múltiples instituciones de gobiernos y organismos no gubernamentales alrededor del mundo, de estos últimos

y entre los más destacados están: Alfa-Redi (Latinoamérica y el Caribe), Amnesty International USA (EE.UU.), Big Brother Watch (Reino Unido), Electronic Frontier Foundation (EE.UU.), Electronic Privacy Information Center - EPIC (EE.UU.), Free Network Foundation (EE.UU.), Human Rights Watch (EE.UU.), Privacy Activism (EE.UU.) y, Wikimedia (EE.UU.).

Al señalarse a los Estados Unidos de América como el principal actor en el espionaje a granel, en las más recientes noticias expuestas a la luz pública, fue imperativo examinar fuentes doctrinales, normativa y jurisprudencia de este país a través de bibliotecas electrónicas y publicaciones de varias universidades, entre las más consultadas, la Universidad de Cornell, Universidad de Yale, Universidad de Harvard, Universidad de Michigan, Universidad de Columbia y Universidad de Georgetown.

Desde luego también se acudió a fuentes tradicionales para obtener el material bibliográfico y documental. Respecto de la información costarricense y española se consultaron las bibliotecas de la Universidad de Costa Rica, la Universidad Autónoma de Centroamérica, la Universidad Escuela Libre de Derecho, de la Asamblea Legislativa y de la Corte Suprema de Justicia. También se consultaron las páginas oficiales para obtener la normativa como la del Boletín Oficial Español (BOE), para la normativa española, como la normativa obtenida del Sistema Nacional de Legislación Vigente (SINALEVI) y la Asamblea Legislativa, para la normativa costarricense. De otra parte, se visitaron las páginas oficiales de los Tribunales españoles y costarricenses para buscar y obtener las sentencias. De esta manera, se también se consultaron múltiples servicios informativos, de los cuales se deja referencia al pie de página.

Por último, ha de advertirse que todo subrayado en el texto es un hipervínculo electrónico que remitirá a una fuente externa de consulta en Internet o, en el caso de "*infra*" o "*supra*", remitirá a un lugar particular de este documento, pues estos subrayados no fueron utilizados con el propósito de resaltar y en su lugar se utilizó la letra negrita, cursiva u otro tamaño de letra. Así mismo, en las citas utilizadas en

la investigación se omitió hacer referencia a la fecha de consulta, tal y como de forma tradicional se suele señalar en los trabajos de investigación, en su lugar, se corroboraron que todos los enlaces fuesen funcionales al 10 de noviembre de 2015, siendo innecesario hacer la referencia en cada una de las citas de páginas web.

3.2. Objetivo general[27].

- Analizar la situación jurídica de los programas de vigilancia masiva, utilizados por algunos Estados, con la colaboración de las empresas privadas de Internet, para demostrar la vulneración de los derechos fundamentales de las personas protegidos en la normativa de Derechos Humanos, tales como el derecho de intimidad, la protección de datos personales, la inviolabilidad de las comunicaciones, afectando con ello el desarrollo de la vida privada de las personas.

3.3. Objetivos específicos.

- Resaltar la importancia de la intimidad como valor para el desarrollo de los seres humanos, considerando el origen histórico cultural.
- Detallar sobre la naturaleza jurídica del Derecho de Intimidad y su desarrollo jurídico, con el propósito de examinar los derechos derivados y la protección jurídica.
- Advertir sobre la afectación y vulnerabilidad de ciertos derechos fundamentales con relación al desarrollo tecnológico, principalmente, con el uso de Internet y servicios relacionados, con el fin de sensibilizar sobre el impacto en la sociedad.
- Exponer sobre los sistemas jurídicos de protección de los datos personales para verificar la efectividad de estos en un mundo globalizado.
- Analizar la legalidad y repercusiones jurídicas producidas por la utilización de programas de vigilancia masiva por parte de las

[27] Actividades basadas en la "Taxonomía de Benjamín Bloom de 1948" como herramienta para establecer los objetivos de aprendizaje. Al efecto se pueden consultar numerosas páginas en las cuales existen una lista de verbos actualizada a la era digital.

agencias de inteligencia. Lo anterior con la finalidad de determinar la posible afectación de los derechos fundamentales de las personas y examinar diversas propuestas.

SEGUNDA PARTE. SOBRE EL DERECHO DE INTIMIDAD.

CAPÍTULO II. LA INTIMIDAD COMO VALOR O CONCEPTO.

"La privacidad de una persona ya no es un tema individual."[28]

[28] Harold "Hal" Abelson, PhD. Profesor de Ingeniería Eléctrica y Ciencias de la Computación del Instituto Tecnológico de Massachusetts.

1. CONSIDERACIONES PRELIMINARES.

El Derecho a la Intimidad se destaca entra los derechos fundamentales a la personalidad y ha sido reconocido desde el siglo XIX, con anterioridad a los derechos sociales, por lo cual se podría ubicar en la primera generación de los derechos humanos. A partir de este derecho se construyeron diversos mecanismos de protección, sirviendo como base de la protección de los datos personales.

Es por ello que, en la actualidad, el estudio del derecho a la intimidad cobra relevancia frente a los avances tecnológicos, que en apariencia hace a los individuos más vulnerables a las intromisiones en su vida privada y por consecuencia en su intimidad.

En términos generales y a lo largo de este trabajo, se expondrá sobre las incidencias de las tecnologías en el Derecho de Intimidad. En un primer apartado de este capítulo, se abordan aspectos conceptuales del vocablo intimidad, debido a que se trata de un término de muy difícil delimitación por su contenido cambiante, así mismo, se advertirá sobre conceptos similares que muchas veces se utilizan como sinónimos de intimidad, tales como: privacidad, secreto, confidencialidad, reserva y otros.

Por sus características particulares, las tecnologías de información y comunicación han incidido en la sociedad, creando la necesidad de que el Derecho intervenga para regular las actividades humanas electrónicas. Al estimarse que el Derecho regula la vida de las personas en sociedad, utilizando un conjunto de normas (Derecho objetivo), hace pensar en que en la mayoría de sociedades actuales o modernas se hable de la regulación para el uso de estas tecnologías.

La incidencia directa de tecnologías de información y comunicación y, particularmente, Internet afecta los derechos fundamentales de las personas. Esta afectación podría ser positiva o negativa. En el primer caso, de forma positiva, cuando se ejercitan libertades como la de expresión e información; en el segundo

caso, de forma negativa, cuando esos derechos son afectados, arbitrariamente, por parte de los poderes públicos o terceros. A esto se dedicará una sección de este capítulo, que incluye un breve análisis de los derechos de la sociedad de la información o sociedades electrónicas.

Antes de avanzar en el tema del derecho de intimidad, se estima necesario hacer unas consideraciones relacionadas con los términos utilizados en la práctica jurídica como sinónimos de este importante derecho, situación que tiende a confundir y entorpecer la administración de justicia y la tutela efectiva de estos derechos.

2. INTIMIDAD Y PRIVACIDAD, ¿AMBAS CARAS DE UNA MISMA MONEDA?

Conviene examinar algunas acepciones terminológicas, pues en la doctrina parece que existe una discusión importante sobre la utilización de los términos de intimidad y privacidad como sinónimos. Los estudiosos de la materia se han dedicado a desarrollar trabajos que han servido de base para muchos otros en ese sentido. Por lo anterior se estima conveniente hacer una breve referencia sobre dichos términos, con el propósito de precisar y facilitar el estudio propuesto.

El contenido de los conceptos de intimidad y privacidad parecieran ser cambiantes en la heterogeneidad cultural que compone a la humanidad, así como, en el devenir histórico. Algunas personas de sociedades aisladas geográficamente, perciben como intimidad y privacidad algo distinto a lo que entienden las personas de los centros urbanos, de la misma forma que, actualmente, no son bien vistos los sanitarios de la antigua Roma, utilizados a la vez por varias personas, unas al lado de otras.

En la doctrina existe gran discusión sobre si el concepto de intimidad es sinónimo de privacidad. Varias legislaciones no advierten diferencia alguna cuando se refieren a uno u otro y, en ambos casos, se refieren al mismo concepto[29]. El término de privacidad es uno de los más difundidos por los medios de comunicación

[29] Para citar un ejemplo del uso de ambos términos como sinónimos, se puede consultar el ATC 642/86, de 23 de julio, el cual señala en su fundamento jurídico 3º que *"el derecho a la intimidad constitucionalmente garantizado por el art. 18 en relación con un área espacial o funcional de la persona precisamente en favor de la salvaguarda de su **privacidad**, que ha de quedar inmune a las agresiones exteriores de otras personas o de la Administración Pública…"*

y uno de los más discutidos por los especialistas en temas normativos de la lengua[30].

La publicación de Díaz Rojo[31] se considera como uno de los principales aportes para delimitar las diferencias conceptuales entre privacidad e intimidad, servirá de guía en este apartado y se compararán los estudios realizados por otros juristas como Tornabene, Nebrera, Agustina y Altman y Taylor. Según Díaz Rojo "El hecho de que una unidad léxica esté registrada en un diccionario, sea este diccionario descriptivo o normativo, es un indicio de que es correcta, y, por tanto, de que puede emplearse sin incurrir en un error"[32].

En el DLE, se define el término de privacidad como "*ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*"[33]. Esta obra recoge la

---

[30] El término *privacidad* es utilizado con mucha frecuencia en la doctrina y jurisprudencia como equivalente de *privacy*, ambos para referirse a la protección de la vida privada, en la que se incluyen el derecho al honor, la intimidad personal y familiar y la propia imagen, suponiendo que estos términos hacen referencia a la esencia de la personalidad, un ámbito reservado de carácter personal alejado de las injerencias de terceros.

[31] DÍAZ ROJO, J. A., *Privacidad: ¿neologismo o barbarismo?* [en línea], Consejo Superior de Investigaciones Científicas, 2002, https://pendientedemigracion.ucm.es/info/especulo/numero21/privaci.html

[32] *Ibíd.*

[33] Respecto de los adjetivos derivados del término, el *Diccionario de la Lengua Española*, señala: *"Que se ejecuta a vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia alguna", "Particular y personal de cada individuo" y "que no es propiedad pública o estatal, sino que pertenece a particulares".* Nótese que se trata de un diccionario descriptivo y no normativo, las confusiones que se presentan suelen darse por tratarse del diccionario oficial de la lengua. *Diccionario de la Lengua Española* (DLE) [en línea], 23ª ed., 2014, http://www.rae.es/recursos/diccionarios/drae. Para Santos Cifuentes, dentro del concepto de *vida privada*, además de lo secreto, es todo lo que compone y construye para sí en soledad el individuo, es decir, aquellas parcelas más ocultas de su ser y de su actividad, ignoradas e impenetrables para los demás en general y que solo ha comunicado a un individuo a un individuo o a muy cercanos allegados, sino también, un espacio menos restringido, ya que abarca lo reservado o confidencial propio de la convivencia social y en compañía con el selecto grupo de personas que lo rodean habitualmente, concepto que, al considerarse en la sociedad histórica donde vive, está en gran medida condicionado por los factores morales y socio-políticos

característica de que la privacidad es una dimensión del ser humano que es objeto de protección jurídica, pues disfrutamos del derecho de que nadie se entrometa en su ámbito.

El término "privado" se origina del latín *privatus,* lo que significa privar y está muy relacionado con la propiedad, propiedad privada, zona privada, uso privado, acceso privado, mensaje privado, reunión privada, todo esto para señalar lo contrario a lo público. El concepto de privacidad también se refiere al aislamiento físico del individuo, un derecho a estar solo y a no ser perturbado por otros en un ámbito determinado, concepto que fue desarrollado, como se indicó en el derecho anglosajón.

Por su origen (neologismo o extranjerismo), algunos han rechazado el uso de la palabra privacidad, por estimar que se trata de una simple traducción del inglés *privacy* y sugieren que se reemplace por el término intimidad[34] o vida privada y, quienes sostienen esta opinión, consideran que tanto intimidad como vida privada son sinónimos preferibles al término privacidad, derivado del inglés[35]. Desde ahora

---

característicos de esa convivencia, CIFUENTES, S., *El derecho a la vida privada, tutela a la intimidad,* ed. La Ley, Buenos Aires, 2007, p. 09.

[34] El DLE define intimidad como: *"Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"*.

[35] TORNABENE, I., "Privacidad e intimidad: la protección legal del información personal en la República Argentina", en AMOROSO FERNÁNDEZ, Y., (dir.), *Género, Código de Juventud: construir sociedades más justas e inclusivas*, Unión Nacional de Juristas de Cuba, 2014, p 87; El *libro de estilo* de El país, en la versión publicada por Santillana, en el año 2002, rechazaba el concepto de privacidad, por considerarla un barbarismo o un anglicismo innecesario fácilmente sustituible por intimidad o vida privada. La última edición de esta publicación señala que: "esta palabra se incorporó al Diccionario académico en el año 2001, y su uso extendido uso se debe probablemente a traducciones defectuosas del inglés *privacy*, que puede tener varios equivalentes en español: intimidad, confidencialidad, soledad, aislamiento, vida privada. En español se ha venido plasmando la diferencia entre los ámbitos "público", "privado" e "íntimo", pero la palabra "privacidad" invade las casillas de los dos últimos. De hecho, la definición académica podría equivaler a "intimidad", pues el Diccionario dice en la entrada de "privacidad": "ámbito de la vida privada que se tiene derecho a

debemos advertir que en algunos países se tutelan ambos derechos por separado y en la doctrina jurídica se han desarrollado estos conceptos con algún grado de relación.

Si lo privado se refiere a un ámbito, a un espacio o a la propiedad sobre algo, no podría entenderse como sinónimo de intimidad. Si se toman los ejemplos señalados unas líneas atrás, puede observarse que se cambia el sentido semántico cuando se sustituye *privacidad* por *intimidad*: propiedad íntima, zona íntima, uso íntimo, acceso íntimo, mensaje íntimo, reunión íntima. Entonces los conceptos de privado e íntimo no parecen ser sinónimos.

Cuando se refiere a intimidad, se trata de las cosas más profundas e interiores de la persona, que suelen ser reservadas. La intimidad es el conjunto de sentimientos, pensamientos e inclinaciones más guardados en el interior -la ideología, la religión o las creencias-, las tendencias personales que afectan a la vida sexual, determinados problemas de salud que se desea mantener en total secreto, u otras inclinaciones, como conductas, hábitos, vicios, etc.[36]

Se debe señalar que, cuando se expone sobre el tema de protección de datos como derecho fundamental, se tiende a igualar los términos de “intimidad” y “privacidad”, para ser utilizados indistintamente. Sin embargo, estos dos términos

---

proteger de cualquier intromisión”. Y, en “intimidad” señala: “Zona espiritual íntima y reservada de una persona o de un grupo, especialmente, la familia”, sin referirse a protección alguna”. Concluye que se puede utilizar la palabra y hace la advertencia de estilo para diferenciar entre los tres ámbitos. *Vid.* El País, *Libro de estilo: nueva versión actualizada*, 22ª ed., Madrid, 2014, [versión para lector digital Kindle].

[36] AGUSTINA SANLLEHÍ, J. R., *Privacidad del trabajador versus deberes de prevención del delito en la empresa,* Editorial B de F, Buenos Aires, 2009, p. 8. Puede decirse que la noción de intimidad se refiere a una esfera mucho más interna, en tanto que la privacidad abarcaría una franja intermedia entre el ámbito estrictamente personal o individual y el espacio donde tiene lugar la actividad pública de la persona, es decir, donde existen relaciones interpersonales, pero sin que se planteen como abiertas al conocimiento público. *Cfr.* NEBRERA GONZÁLEZ, M. (coord.), *Intimidad y seguridad: dos conceptos y un conflicto.* Associació Isegs per a la Promoció dels Estudis sobre la Governabilitat, Barcelona, 2002, p. 17.

tienen un alcance distinto que es necesario conocer para saber dónde empiezan y acaban el derecho a la intimidad, a la privacidad y a la protección de datos de carácter personal.

Lo íntimo es un adjetivo que proviene del latín *intimus* y que alude a lo interior, a lo interno, a lo recóndito, que está en el fondo de algo. Hace referencia a aquello que queremos ocultar de los demás, que queremos preservar sin que se vea, que únicamente destinamos a nosotros mismos y a quienes elegimos. El propio DLE define "íntimo" como "*lo más interior o interno", y el término "intimidad" como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia*".

Ahora bien, cuando se agregan términos como secreto, confidencialidad, reserva, pareciera que se trata, de igual forma, como sinónimos. En la normativa penal suele indicarse que las comunicaciones son secretas, para indicar que son libres de interferencias por parte de terceras personas, pero será igual si se señala que las conversaciones son privadas, íntimas, confidenciales, personales o secretas.

La diferencia, evidentemente, es conceptual, como ya se aprecia, por ello es de cuidado determinar qué concepto es el indicado en razón de la protección que se quiere dar a estos derechos, dado que no significan lo mismo. Rápidamente se puede indicar que las comunicaciones son personales, íntimas o confidenciales, sin embargo, podrían ser públicas al mismo tiempo, es decir, contrarias a lo privado. Esto mismo ocurre cuando se habla de protección de datos, esos datos podrían ser privados, personales, íntimos, secretos, reservados o confidenciales.

Inés Tornabene concluye que es necesaria una distinción entre ambos conceptos (privacidad e intimidad), distinción que estima es solo una cuestión de grado dentro de esta especie (una relación de género-especie); indica que la intimidad pertenece al ámbito de la privacidad, todo lo íntimo es privado, en cambio

no toda la información privada es información íntima[37]. La conclusión de la citada autora pareciera muy razonable, sin embargo, en su premisa no explica, con ese supuesto, qué ocurriría cuando algo íntimo se convierte en público, puesto que aun así no pierde el carácter de íntimo, por lo que no resulta cierto que todo lo íntimo es privado, si se omite la palabra "*todo"* en el primer enunciado se estaría de acuerdo con la autora.

En síntesis, se podría decir que, morfológicamente, *privacidad* nace del inglés *privacy* y del francés *privacité,* y se refiere a un término aceptado en los sistemas del lenguaje español como un neologismo. Sin embargo, semánticamente, el concepto de *privacidad* no es sinónimo de *intimidad*.

De otra parte, se estima que la noción de privacidad utilizada en EE.UU. no puede equipararse con la concepción de intimidad utilizada en América Latina y Europa, lugares en los que intimidad parece tener un carácter más restringido que el término privacidad cuyo contenido es más extenso, al identificarse con el ámbito de la vida privada para protegerse de cualquier intromisión. [38]

La confidencialidad implica el hecho de no dar publicidad o transmitir a terceros datos e informaciones reservadas; la intimidad es lo más interno del sujeto, sus sentimientos y pensamientos profundos; la privacidad está constituida por las facetas que forman la vida personal, frente a la dimensión pública o profesional. Los asuntos íntimos son privados, pero no todos los aspectos privados son íntimos.

---

[37] TORNABENE, I., *op. cit.,* p. 100.

[38] Altman y Taylor desarrollaron una teoría sobre la penetración social y sostienen que la comunicación interpersonal se desarrolla por fases sucesivas, que van superando diferentes capas de entrañamiento, pero que no necesariamente agotan el proceso de profundización comunicativa. Como metáfora de la teoría de la penetración social, emplean la cebolla y sus capas, que rodean el núcleo más profundo de la intimidad personal. ALTMAN, I., y TAYLOR D. A., *Social penetration: The development of interpersonal relationships*, Holt, Rinehart and Winston, Nueva York, 1973.

Una aproximación al concepto de intimidad ha permitido observar que se trata de un valor que antecede su reconocimiento como derecho. De esta manera el concepto de intimidad es proteiforme, pues varía según la cultura, la región y el devenir histórico. Lo que percibe en algunas áreas geográficas como intimidad pareciera ser distinto a lo que se entiende en otras. Se pueden identificar culturas y costumbre individualistas, también existen otras en las cuales los sujetos comparten con la colectividad, de forma dependiente, una gran cantidad de las actividades cotidianas.

Entre las primera conclusiones se expone la diferencia entre privacidad e intimidad, reconociendo el primero como un término derivado de privacy el cual es aceptado en los sistemas del lenguaje español como neologismo. Adicionalmente, se debe advertir que estos conceptos tienen connotaciones semánticas distintas. El concepto de intimidad se refiere a las cosas más profundas e interiores de la persona, que suelen ser reservadas, mientras que lo privado significa privar y está relacionado con la propiedad como propiedad privada, zona privada, uso privado, acceso privado, mensaje privado, reunión privada, lo anterior para señalar lo contrario a lo público. Pese a lo anterior, cuando hablamos de derechos, en los sistemas jurídicos anglosajones el derecho reconocido es el right to privacy, mientras que en el derecho continental es el derecho equivalente es el derecho de intimidad. Si se hace una traducción literal refiriéndose al derecho de los angloparlantes se debería indicar como el derecho de privacidad y, en el caso contrario, lo correcto es denominarlo como derecho de intimidad. En De otra parte cuando no se hable del derecho sino de la intimidad y la privacidad, debe advertirse que un concepto es distinto al otro, y si bien ambos son aceptados en el idioma español dentro del concepto de privacidad se puede ubicar el concepto de intimidad, como una relación de género-especie.

En los siguientes apartados de este trabajo se hará referencia a los términos de derecho de privacidad o derecho de intimidad dependiendo de autores citados, o del sistema jurídico al cual se hace referencia. En el derecho de *common law* lo

correcto será utilizar el término de derecho privacidad y, en el derecho continental lo más conveniente será emplear el término de derecho intimidad, aunque se advierte que algunos autores, la jurisprudencia e incluso en las leyes refiere al derecho de privacidad como sinónimo de derecho intimidad.

Ahora bien, tal y como se advirtió *supra* en este apartado, sobre los términos de privacidad e intimidad, podría entenderse que ambos conceptos, en algunos contextos, pueden y son empleados como sinónimos, de ahí que en la presente investigación se hará referencia a ambos conceptos cuando no haga referencia al derecho, pues en ese caso, se utilizará el término de derecho de intimidad para el sistema del derecho continental y el término de derecho de privacidad o *privacy* para el sistema de derecho anglosajón.

3. DESARROLLO HISTÓRICO DEL DERECHO DE PRIVACIDAD E INTIMIDAD.

3.1. Origen del concepto de intimidad.

En las primeras conceptualizaciones de la intimidad, se asocia con la soledad del individuo con el aislamiento físico de la comunidad. En esta aproximación al concepto, conviene advertir que este puede hacer referencia a una condición o fenómeno, una aspiración, un reclamo o idea o bien al derecho de intimidad. Ciertamente, en cualquier de estas referencias se encuentran en las sociedades presentes y del pasado.

Las anteriores aproximaciones sirven para observar y comparar la evolución de la intimidad como derecho. Sin embargo, antes de este reconocimiento por parte del derecho positivo, se presentaba como un instinto, reconocido en el propio ser como parte de su dignidad. Incluso, algunos autores señalaban la existencia de la intimidad como un fenómeno del reino animal, basado en el instinto de territorialidad.

Se estima conveniente, antes de que se exponga sobre el origen y desarrollo del concepto de intimidad, se indique que cuando se habla de intimidad se puede hacer referencia a una condición (fenómeno), una aspiración, un reclamo (idea) o un derecho[39]. Estas, podrían ser etapas del desarrollo del derecho de intimidad, que

[39] Carlos Ruíz Miguel señala que *"La intimidad puede ser contemplada desde una triple perspectiva: como fenómeno (factor socio-económico), como idea (factor cultural) y como derecho (factor político-jurídico)".* RUIZ MIGUEL, C., "La configuración constitucional del derecho a la intimidad", *Tesis doctoral,* Universidad Complutense de Madrid, 1992, p. 3.

se han dado de forma progresiva, sin que se puedan determinar en el tiempo y espacio de forma precisa.

Para Alan Westin[40], profesor de la Universidad de Columbia, la privacidad se define como un reclamo, aunque también la reconoce como una condición de aislamiento del individuo de la sociedad. Ambas consideraciones las percibe como una clasificación entre privacidad como estado, como idea consciente y la privacidad como derecho.

Desde la perspectiva de la intimidad como fenómeno, Ortega y Gasset distingue las esferas de la vitalidad, el alma y el espíritu y señala que la intimidad es un fenómeno, un hecho, no una hipótesis metafísica.[41] Esa idea, se plantea de igual manera por Westin, quien afirma que *"ciertos aspectos de la intimidad se encuentran prácticamente en todas las sociedades del presente y el pasado"*[42], incluso este autor describe que podría existir la intimidad como fenómeno en el reino animal, basado en el instinto de territorialidad, lo que reafirmaría que se encuentre en cualquier sociedad.

Con respecto al origen de la intimidad como idea, se podría entender que los individuos realizan actos que se traducen en un ejercicio de la intimidad, pero ello no significa que hayan tomado conciencia de esta. La intimidad está presente, de forma inconsciente, en todas las sociedades como instinto, sin embargo, aún en las sociedades que está presente de forma consciente el grado de teorización es variable.

---

[40] WESTIN, A., *Privacy and freedom*, Atheneum, New York, 1967, p. 3.

[41] RUIZ MIGUEL, C., *op. cit.,* p. 3.

[42] WESTIN, A., *op. cit.,* p. 6.

Desde el ámbito jurídico existe en la doctrina una cantidad de trabajos que pretenden teorizar sobre el concepto de intimidad como derecho. Además, se observan una gran cantidad de normas protectoras de las esferas de la intimidad, en las que se teoriza sobre el concepto. Sin embargo, en la mayoría de los casos se necesitará atender a la intimidad como fenómeno o a la idea para así comprender su aspecto jurídico.

Algunos autores consideran que los orígenes jurídicos del derecho de intimidad se remontan al derecho anglosajón[43], sin embargo, existen otros que estiman que ese valor se asocia a dos vertientes previas, el cristianismo y su modalidad reformista a finales de la edad media ligada a la desaparición de la sociedad feudal, y de otra parte con la Revolución Francesa y el eventual surgimiento de la burguesía capitalista, quienes tenían la posibilidad económica y social de apartarse de la sociedad.

Desde la tesis iusnaturalistas se explica el paso de los derechos personales a los derechos fundamentales como la materialización del valor de la dignidad humana. Mientras que la tesis positivista no concibe reconocer derechos fundamentales que no se hallen, expresamente, consagrados en una Carta constitucional.

En torno al problema del origen de la intimidad como idea o valor, se han formulado dos teorías principales, la racionalista y la histórica. La primera, sitúa el génesis de este derecho en el período de racionalismo y de la ilustración como consecuencia de la creciente burguesía. Por su parte, en el caso de la segunda

[43] Existe casi unanimidad en la doctrina al aceptar la obra de Warren y Brandeis “The right to privacy” como el origen jurídico del término de privacidad.

teoría, la histórica, se remonta más atrás en la historia para buscar el origen del concepto.[44]

Para Pérez Luño, la intimidad nace como una facultad de la burguesía[45]. Se trata de un privilegio de las altas esferas sociales, en su mayor parte, la nobleza, quienes tenían la posibilidad de aislamiento por libre elección[46]. A medida que crecen los núcleos urbanos y aparecen las formas de división del trabajo se marca la diferencia de quienes habitan en una inmueble privado o los que habitan en el establecimiento en que trabajan. Esto hace que exista la necesidad de proteger un espacio determinado, un espacio privado. En la tesis sostenida por el citado autor[47], podría decirse que se distingue entre la intimidad como idea y como derecho, sin embargo, en esa opinión pareciera que ambas surgen con la burguesía capitalista.

En la mencionada tesis la intimidad se configura como una aspiración de la burguesía de acceder a lo que había sido un privilegio de unos pocos y de esa manera se conforma la idea moderna de intimidad. De este modo, la vinculación entre la propiedad privada y el derecho de privacidad no es puramente jurídico-formal, sino que la propiedad sirve de condición para lograr el aislamiento.[48]

---

[44] RUIZ MIGUEL, C., *op. cit.,* p. 7.

[45] PEREZ LUÑO, A. E., *Derechos Humanos, Estado de Derecho y Constitución,* Editorial Tecnos S.A., Madrid, 5ª ed., 1995, pp. 322-323.

[46] KONVITZ estima que en el cristianismo se origina la idea de la intimidad como valor, en ese sentido afirma que, en La Biblia, en el libro del Génesis aparece una temprana referencia del concepto, cuando narra que Adán y Eva, luego de comer del fruto del árbol del conocimiento, se enteran de su desnudez y se cubren. *Cfr.* KONVITZ, M.R., "Privacy and the Law: a Philosophical Prelude", 31 *Law & Contemp*, Probos, 1966, p. 272-276.

[47] PEREZ LUÑO, A. E., *Derechos Humanos, Estado de Derecho..., op. cit.,* pp. 322-323.

[48] *Ibíd.*

La tesis racionalista, ha sido sostenida por Berlín y Béjar[49], para quienes el nacimiento de este concepto se remonta al Renacimiento, tomando su sentido actual durante la Reforma a través de la noción de *fuero interno*.

Por su parte -la teoría histórica- afirma que el origen de la intimidad se remonta a la Europa de la Ilustración, ubicando su desarrollo histórico en un breve instante temporal y geográfico[50]. Esta teoría se basa en dos tesis principales, la primera relacionada con la propiedad burguesa, al igual que la tesis racionalista. Esto es similar a lo que indicaba Westin[51], respecto a la intimidad en el reino animal, con relación a la territorialidad (propiedad en los humanos), lo que no nace con la burguesía, sino con el ser humano.

Deben reconocerse otros períodos anteriores del desarrollo de la intimidad como concepto, como resulta ser el caso de la antigua Grecia, donde el concepto de la *polis* no dejaba espacio al entendimiento de la intimidad, como existencia reservada de la vida personal del ser humano. Sin embargo, podría señalarse, que aparece tal conceptualización con el desarrollo de la idea consciente de la intimidad, es decir el alma y podría adjudicarse ese concepto a Sócrates, quien separaba lo interno de lo externo, lo interno como secreto privado, elemento de la intimidad[52].

---

[49] BÉJAR, H., "La génesis de la privacidad en el pensamiento liberal" en *Sistema,* No. 76, enero 1987, p. 59-65; BERLÍN, I., "Dos conceptos de libertad", trad. BAYÓN, J., en *Cuatro ensayos sobre la libertad,* Alianza, Madrid, 1988, p. 187-199.

[50] ROSA VELÁZQUEZ, L.D., "Panorama General del Derecho a la Intimidad", en *Revista Jurídica Universidad de Puerto Rica,* vol. 72.4, 2002, pp. 666-670.

[51] WESTIN, A., *op. cit.,* pp. 8-12.

[52] REBOLLO DELGADO, L., *El derecho fundamental a la intimidad,* Dykinson, Segunda edición, Madrid, 2005, p. 55.

De otra parte, en la antigua Roma[53], Séneca, profundizó en los trabajos de Sócrates, influido por el estoicismo, expresa en sus obras la contraposición entre el hombre inmerso en los negocios y ocupaciones exteriores y el hombre que vive retirado e inmerso en la *sapientia*[54]*.* Ese antagonismo entre el hombre interior y exterior es un elemento que podría ser considerado como constitutivo de la idea actual de intimidad, ubicando a Séneca[55] como precursor del concepto de intimidad.

Para Ruiz Miguel, San Agustín fue el primer autor en teorizar sobre la intimidad, como idea central a lo largo de los títulos del autor. En sus obras, los vocablos de raíz latina *intimus* se emplearon en el mismo sentido del vocablo actual[56].

En el derecho de la época medieval, se aprecian regulaciones relacionadas con la inviolabilidad del domicilio, defensa del patrimonio, sin alguna presencia de la parte subjetiva o relacionada con la vida íntima de la persona[57].

---

[53] Las primeras manifestaciones históricas de protección de la intimidad se producen en el Derecho Romano en relación fundamentalmente con el honor de las personas, la protección del domicilio o la libertad religiosa. *Cfr*. REBOLLO DELGADO, L., *op. cit.,* 2005, pp. 55-56.

[54] *Vid.* RUIZ MIGUEL, C., *op. cit.,* p. 27-29; *v.et.* ROSA VELÁZQUEZ, L.D., *op. cit.,* p. 670.

[55] Otra prueba del origen del concepto de intimidad utilizado en la antigua Roma, lo es la utilización de *intimus.* Este término tiene dos acepciones, en primer lugar, hace referencia a lo interior o el fondo de algo (Cicerón lo utilizó para referirse al domicilio) y, en segundo lugar, se refiere a los familiares o amigos íntimos. *Cfr.* RUIZ MIGUEL, C., *op. cit.,* p. 27-29.

[56] El autor citado afirma que la idea de intimidad se perfecciona en el texto de San Agustín y este es el primero en hacer una exploración completa y sistemática de la intimidad. RUIZ MIGUEL, C., *op. cit.,* p. 27-29.

[57] *Vid. Decreta de la Curia Regia* de 1188, [en línea], http://www.mecd.gob.es/cultura-mecd/areas-cultura/archivos/novedades/documentos-novedades/3.html

Algunos autores afirman que, el derecho a la intimidad se incluye entre los derechos llamados personalísimos, es decir, todos aquellos que los seres humanos tienen por el hecho mismo de existir, tales como: el derecho de nacer, derecho de vivir, derecho al cuerpo, derecho a la libertad, derecho al nombre, derecho al honor, derecho a la propia imagen, y en cuanto a este trabajo concierne, derecho a la intimidad[58], puesto que, como todos los derechos humanos, este derecho deriva de la dignidad humana. Debido a que este concepto fue desarrollado desde el siglo XIX, se ubica en la primera generación de derechos humanos, antes que se desarrollaran los derechos sociales.

[58] *Vid.* SCHLAIN, N. B., *Internet y el derecho a la intimidad,* Editorial académica española. 2012. p. 9.

3.2. Origen anglosajón del derecho a la *privacy*.

Para la mayoría de los autores, el desarrollo doctrinal del derecho de intimidad se origina en EE.UU., con el famoso ensayo de Warren y Brandeis, que se comentará más adelante. Lo cierto es que como concepto o idea fue desarrollado con anterioridad, incluso, algunos autores afirman que este se origina con el surgimiento del ser humano, como se indicó desde el primer apartado de este capítulo *supra*.

El origen del concepto jurídico del derecho de intimidad en EE.UU. se ubica 1873, con la publicación de la obra *"The Elements of Torts"* del Juez Thomas McIntyre Cooley, que lo definió como *"the right to be let alone"*[59], es decir, el derecho a ser dejado en paz, o a ser dejado sólo.[60]

Este derecho se encuentra implícito en la Constitución de Estado Unidos y fue reconocido, inicialmente, por la Suprema Corte de Justicia. En la Constitución estadounidense de 1787, ni en sus enmiendas se reconoce, de forma expresa, el *derecho de privacidad*, por lo menos como *right to privacy*. Este derecho fue reconocido en la jurisprudencia y se desprende de otros derechos reconocidos,

---

[59] El derecho a no ser molestado significaba, en esa época, no sólo un factor negativo, sino también uno positivo, basado en impedir la circulación de fotografías de una persona (la fotografía, se consideraba un invento mecánico que invadía la vida privada de las personas) sin consentimiento del titular. Esos planteamientos, fueron plasmados judicialmente, como lo asevera Elvira López Díaz, al decir que "Tres años más tarde de la publicación de este conocido artículo un Tribunal utilizó por primera vez la expresión acuñada por los dos abogados, Warren y Brandeis, fue el caso Marks v. Joffa, fallado por el Tribunal de New York: el demandante, un actor y estudiante de leyes, había visto un retrato suyo publicado en un periódico propiedad del demandado, formando parte de un concurso de popularidad, al que se le oponía personalmente. La sentencia, estimó la demanda y declaró su *derecho a ser dejado en paz*, basándose en el hecho de que ningún periódico o institución tiene derecho a usar el nombre o la fotografía de nadie, sin su consentimiento. *Cfr.* LÓPEZ DIAZ, E., *El derecho al honor y l derecho a la intimidad*, Ed. Dykinson, Madrid, 1996, p. 175.

[60] THOMAS McINTYRE, C., *The elements of torts,* Callaghan and Company, 1895, *s.n.*

como en el caso de la primera enmienda del derecho de asociación y en el caso de la cuarta enmienda frente a los registros personales y domiciliarios. La décimo cuarta enmienda tutela los derechos relativos a la información personal *"informational privacy".*[61] Principalmente, su protección se origina en el derecho civil, como agravios contra la privacidad, sin embargo, existen otras leyes que regulan derechos relacionados con la privacidad, los cuales serán abordados a lo largo de la investigación.

En 1890, luego de la obra del Juez Thomas McIntyre, Warren y Brandeis, publicaron "*The right to privacy",* obra en la que desarrollan las bases jurídicas de la noción de *privacy,* como derecho a la soledad, como la facultad "*to be let alone*".[62] A partir de ese momento se inició un gran desarrollo doctrinal, basado en la jurisprudencia que con posterioridad sería expuesta por Brandeis como juez del tribunal supremo.

Como se indicó, entre las primeras obras en teorizar este derecho se encuentra la obra de Warren y Brandeis titulada "The Right to Privacy" de 1890. Sin duda, ha sido la obra más desatacada y comentada como origen del derecho a la privacidad en los EE.UU. Una anotación importante sobre la obra señalada se debe a que este derecho se reconoce como respuesta y la necesidad de protección frente a los avances tecnológicos de la época y las actuaciones de la prensa. Es muy

---

[61] Para un análisis de la diferente evolución del derecho en el sistema constitucional estadounidense y el europeo, *vid*. WHITMAN, J. Q., "The Two Western Cultures of Privacy: Dignity versus Liberty", en *Yale Law Journal*, vol. 113, 2004, pp. 1151 y ss.; Apunta Julio Maier que como fuente histórica, este principio se remota a la Constitución de los EE. UU. del 17 de septiembre de 1787, en particular a la IV Enmienda, como el derecho del pueblo a: *"estar seguro en sus personas, casas, papeles y efectos, contra inquisiciones o apoderamientos injustos, no se violará, y no se darán órdenes sino en causas probables, sostenidas por un juramento y señalando particularmente el lugar que haya de inquirirse, y los efectos que deban tomarse".* MAIER, J. B.J., *Derecho Procesal,* Buenos Aires, Tomo I, 2ª ed., 1996, p. 679.

[62] WARREN S. D., y BRANDEIS, L. D., "The Right to Privacy", en *Harvard Law Review*, 4, 1890, pp. 193 y sigs., [en línea], http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

probable que el éxito de la obra estuviese relacionado con el caso que resolvió el propio coautor Louis Brandeis como juez de la Corte Suprema en la opinión disidente del caso Olmstead v. United States.

En esa época, Warren y Brandeis, intentaron establecer límites jurídicos que pudieran impedir las intromisiones de la prensa en la vida privada de las personas, bajo una premisa de avanzada para ese momento histórico. Una situación personal llevó a los autores a escribir el artículo, esta estaba relacionada con la esposa de Warren quien fue hija del senador Bayard, los Warren llevaban una vida social activa en la ciudad de Boston, daban fiestas que eran descritas en detalle por la prensa local, particularmente el *Saturday Evening Gazette.* En 1890 fue publicado un artículo sobre una cena realizada en la casa de la familia Warren con motivo de la celebración de un familiar, esta situación le molestó y buscó a su compañero de estudios Brandeis para publicar el artículo que tanta importancia tuvo en el desarrollo del derecho a la intimidad. [63]

Curiosamente, el citado artículo se fundamenta en la contención frente al desarrollo tecnológico de la época[64]. Alegaban que este podría llegar a facilitar agravios o intromisiones sin permitir que el damnificado pudiera contar con ningún remedio o prevención a dicha acción. En la teoría planteada, domina una construcción negativa del derecho, en la medida en que su objetivo era establecer un límite jurídico que vedase las intromisiones de la prensa en la vida privada.

---

[63] *Vid.* FAYOS CARDO, A., *Derecho a la intimidad y medios de comunicación,* Centro de Estudios Políticos y Constitucionales, Madrid, 2000, p. 25; CELIS QUINTAL, M.A., "La protección de la intimidad como derecho fundamental de los mexicanos" [en línea], http://biblio.juridicas.unam.mx/libros/5/2253/9.pdf

[64] El ensayo citado tiene origen a causa de la intromisión de la prensa escrita y el avance tecnológico de mediados del siglo XX. Desde ese momento se aprecia una visión *iustecnológica* por la injerencia de los medios de prensa con la utilización, en ese momento, de las cámaras fotográficas.

Además, manifestaron la necesidad de definir un principio que pudiera ser invocado para proteger la vida privada del individuo frente a su invasión por modernos mecanismos de interceptación o grabación que amenazan con la difusión indiscriminada de información privada.[65]

La concepción del derecho a la intimidad, de carácter contractualista[66], que se podría valorarse como negativa, expresa el contenido original de este derecho, tal como fuera formulado en Harvard en 1890[67]. Adquiriendo vigencia hoy día, con las formulaciones garantistas de los derechos fundamentales, la teorización del

---

[65] Un análisis exhaustivo sobre la historia de los casos estadounidenses sobre el derecho a la privacidad, la opinión disidente y de, finalmente, el reconocimiento jurisprudencial de ese país en: SALDAÑA, M. N., "la protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de información personal en los Estados Unidos" en *Revista Aucaria,* vol. 9, No. 18, Sevilla, 2007.

[66] El principio invocable para la protección de la *privacy,* no es el empleado para proteger el honor, ni el principio que se ha aplicado al amparar estos derechos (los referidos a la propiedad intelectual y artística, en determinados casos de publicación ilegal, los cuales no emanan de un contrato, de una buena fe especial, sino que son derechos *erga omnes*, vale decir, oponibles a todo el mundo: particulares y Estado) no es en realidad el de propiedad privada, por más que esa palabra sea empleada en un sentido amplio y poco usual. *Cfr.* RIASCOS GÓMEZ, L. O., *op. cit.,* p. 14.

[67] "Los recientes inventos y los nuevos métodos de hacer negocios fueron los focos de atención en el siguiente paso que hubo de darse para amparar a la persona, y para garantizar al individuo lo que el juez Cooley denomina el derecho "a no ser molestado". Las instantáneas fotográficas y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña; y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: lo que se susurre en la intimidad, será proclamado a los cuatro vientos […] La intensidad y complejidad de la vida, que acompañan a los avances de la civilización, han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se ha convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales". Casi cuarenta años después, Brandeis defendió estos alegatos como juez del Tribunal Supremo en opinión disidente del caso *Olmstead v. United States* WARREN S. D., y BRANDEIS, L. D., *op. cit.* p. 195-196.

estado mínimo y la limitación de los poderes públicos frente a la esfera de derechos y libertades de los ciudadanos.[68]

En EE.UU. en los cincuenta años siguientes a la publicación del ensayo de Warren y Brandeis, se discutieron cientos de casos ligados a la intrusión en la vida privada por la prensa, la fotografía, la radio y la televisión. Así, el derecho a la privacidad se terminó configurando como un derecho autónomo, cuya protección era indirecta.[69] Además, se reconocieron otros derechos como derivados de este derecho, tales como el derecho al honor, a la imagen, la inviolabilidad del domicilio y las comunicaciones y por último la protección de los datos personales.

Solo algunos años después, en 1905, la Corte Suprema de Georgia, en el caso Pavesick & New England Life Insurance Company, reconoce la existencia del derecho a la propia imagen y el derecho a la intimidad de la vida privada, fundamentado en que ése derecho nace de las leyes naturales y señalando que la libertad personal abarca el derecho a la vida pública tanto como el derecho correlativo a la intimidad. En este caso, el juez Andrew Coob indicó "*la libertad incluye el derecho como uno quiera, en la medida en que no moleste el derecho de los otros o el público. Algunos desean llevar una vida apartada; otros desean vivir una existencia privada en parte y, en otra, una vida pública. Algunos desean una vida de ocupaciones que llame constantemente sobre ellos la atención del público; otros prefieren el estudio de la contemplación, y sólo atraen la atención del público en determinadas circunstancias. Cada uno tiene la libertad para elegir su modo de*

---

[68] *Cfr.* PEREZ LUÑO, A. E., *Derechos Humanos, Estado de Derecho… op. cit.,* pp. 322-324.

[69] ARDÓN ACUÑA, L., "La Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales. ¿Brinda una protección real y efectiva para el derecho a la autodeterminación informativa en Costa Rica?", *Tesis Maestría,* Universidad Nacional de Lomas de Zamora, 2013, p. 16.

vivir, y ningún individuo, ni la sociedad, puede retirarle este derecho, salvo cuando cumplen deberes públicos (v.gr. Servir de jurado de testigo). El que quiera vivir en retiro personal tiene el derecho de elegir los momentos, lugares y circunstancias en que se muestre a los ojos del público"[70].

La sentencia señalada fue considerada como la base del reconocimiento del derecho a la intimidad (*leading case*) en el *common law.* El juez Coob reconoció que el derecho de privacidad derivaba del derecho natural y que no había sido reconocido antes debido al conservacionismo del aparato judicial. También adelantó que una persona podía renunciar al derecho a la privacidad, si se desempeñaba en una ocupación o puesto que demandara la aprobación o patrocinio del público. Sin embargo, el Tribunal Supremo no reconoce ese derecho como independiente hasta el caso Griswold vs. Connecticut de 1965[71], en el que se estima inconstitucional la prohibición de venta de anticonceptivos por vulnerar el derecho a la intimidad y se protege la privacidad de las parejas casadas. En este caso por mayoría se consideró que lo establecido en la Constitución Federal, de conformidad con el criterio del juez Douglas y de conformidad con las enmiendas primera, tercera, cuarta, quinta y novena, de la Constitución se protegía como derecho accesorio de derechos ya reconocidos en el derecho a la privacidad.

Dentro de tales garantías, fue destacada la primera enmienda sobre el derecho de asociación y el derecho a la libertad de conciencia; la tercera, prohíbe en tiempos de paz el acuartelamiento de soldados en cualquier casa, sin el consentimiento del dueño; la cuarta, que afirma explícitamente el derecho de pueblo

---

[70] *Vid.* CIFUENTES, S., *El derecho a la vida privada, tutela a la intimidad*, ed. La Ley, Buenos Aires, 2007, pp. 31-32.

[71] Caso de la *Corte Suprema de Justicia de los EE.UU.* 381 U.S. 479, [en línea], https://supreme.justia.com/cases/federal/us/381/479/case.html

a la seguridad de sus personas, casas, papeles y efectos contra irrazonables secuestros y requisas; la quinta, que en su cláusula de la autoincriminación permite al ciudadano crear una zona de privacidad a la cual el gobierno no puede forzarlo a renunciar contra su voluntad; la novena, que establece que en la enumeración de la Constitución no podrán ser interpretada para negar otros retenidos por el pueblo[72].

A raíz de este fallo, en 1972, se aplicó el caso Griswold vs. Connecticut en la causa Eisenstad vs. Baird[73] y se afirmó que el caso Griswold no solo se refería a la privacidad del matrimonio, pues el derecho de intimidad es un derecho individual, y sin importar si los sujetos son casados o solteros se debe respetar la privacidad de la intromisión estatal.

En EE.UU. el derecho a la privacidad se encuentra en el derecho común (*Common law*)[74], fuera del reconocimiento constitucional, así se entiende que

---

[72] *Vid.* CIFUENTES, S., *op. cit.,* pp. 33-34. El problema central del caso fue una antigua ley de Connecticut que tipificaba como delito el uso de drogas o mecanismos, por parte de personas casadas o solteras, para prevenir la natalidad o incluso que se repartiera información para su uso. Los demás jueces que se unen al criterio para formar la mayoría basan su argumento en la novena enmienda, señalando que esto vulneraba la privacidad del matrimonio, que por su importancia también era afín a la libertad de expresión, religión y reunión.

[73] Corte Suprema de EE.UU. caso 405 U.S. 438 Eisenstadt v. Baird 1972.

[74] *"Contemporary US privacy law is found in the common law, in constitutional law, and in statutes. In a nutshell, US privacy law includes the four common law invasion of privacy torts recognized in most states and by the American Law Institute's Restatement of (Second) of Torts: intrusion upon seclusion, publication given to private facts, false light publicity, and misappropriation of identity. Privacy law includes the common law of publicity and confidentiality, in so far as they protect privacy interests. Next, privacy law includes provisions and interpretations of the federal constitution. Although the word "privacy" does not appear in the US Constitution, a cherished part of the document, the Bill of Rights, has spawned a mountain of privacy protection requirements. The First and Fourth Amendments' jurisprudence of associational, physical, and informational privacy are notable in this regard. The controversial Fourteenth Amendment equal protection and substantive due process decisional privacy jurisprudence is part of privacy law, too. The Third, Fifth, Eighth, and Ninth Amendments have been held to protect privacy interests. Think broadly enough to construe personal lifestyle preferences as privacy interests and even the Second Amendment "right to bear arms" and the Twenty-First Amendment ending national alcohol prohibition start to look like branches of privacy law. Returning from the fringe to the center, privacy law includes state constitutions. State courts have*

cualquiera que invada intencionadamente, física o de cualquier otra forma el aislamiento de otro, en lo que se refiere a sus asuntos privados, queda sujeto a la responsabilidad por invasión de la intimidad (*torts law*). Teniendo en cuenta que este agravio se aplica a un lugar privado, se puede deducir su aplicación a los archivos informáticos guardados en un lugar privado, así la jurisprudencia aplicada a las escuchas telefónicas, y a la intercepción del correo personal, autoriza esta amplia interpretación.[75] En consecuencia, en Internet cualquiera que cometa una intrusión

---

repeatedly held that state constitutions, some with explicit privacy protection provisions, significantly expand privacy protection beyond federal limits. The final major dimension of privacy law consists of the federal and state statutes that protect privacy interests". El derecho de privacidad contemporáneo de Estados Unidos se encuentra en el common law, en derecho constitucional y en los estatutos. En pocas palabras, ley de privacidad de Estados Unidos incluye la invasión de derecho común cuatro de agravios a la privacidad reconocidos en la mayoría de los Estados y por reafirmación del American Law Institute (Second) of Torts: intrusión en reclusión, publicación dada a hechos privados, publicidad falsa luz y apropiación de identidad. Ley de privacidad incluye la ley común de publicidad y confidencialidad, en la medida en que protegen los intereses de privacidad. A continuación, ley de privacidad incluye disposiciones e interpretaciones de la Constitución federal. Aunque la "privacidad" palabra no aparece en la Constitución, una preciada parte del documento, la declaración de derechos, ha generado una montaña de requerimientos de protección de privacidad. La primera y cuarta enmiendas jurisprudencia de privacidad asociativa, físico e informativo son notables en este sentido. El polémico igual protección de la Decimocuarta Enmienda y jurisprudencia sustantiva debido proceso decisional privacidad es parte de la ley de privacidad, también. El tercer, quinto, octavo y noveno modificaciones se han realizado proteger la privacidad de sus intereses. Creo que ampliamente suficiente deducir preferencias de estilo de vida personal como intereses de privacidad e incluso la segunda enmienda "derecho a llevar armas" y los veinte - primera enmienda final prohibición nacional del alcohol empiezan a parecer las ramas del derecho de privacidad. Regreso de la periferia al centro, ley de privacidad incluye constituciones de los Estados. Los tribunales estatales han sostenido reiteradamente que constituciones de los Estados, algunos de ellos con las disposiciones de protección de privacidad explícita, ampliar significativamente la protección de la privacidad más allá de los límites federales. La última dimensión importante de la ley de privacidad consiste en los estatutos federales y estatales que protegen los intereses de privacidad. [traducción libre del autor], ALLEN, ANITA L., *Unpopular Privacy: What must we hide?,* Oxfort University Press, New York, 2011, [versión para lector digital Kindle].

[75] CASTILLO JIMENES, C., "Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información", *En Derecho y Conocimiento*, vol. 1, Facultad de Derecho de la Universidad de Huelva, [en línea], http://www.uhu.es/derechoyconocimiento/DyC01/A02.pdf

ofensiva, puede quedar obligado a compensar a la víctima por la invasión a su intimidad.

Warren y Brandeis, estudiaron la normativa legal existente para buscar amparo a las invasiones de la privacidad. La forma propuesta, fue a través de las leyes de responsabilidad civil (torts law). Los agravios reconocidos por los autores, fueron con posterioridad acuñados por William Prosser en 1960[76].

Estos agravios fueron reconocidos a partir de los problemas de privacidad planteados por Warren y Brandeis. Aunque estos problemas, en un inicio, se reclamaron a raíz de los avances tecnológicos de la época y las actuaciones de la prensa, hoy día se presentan muchas amenazas adicionales a la intimidad que justifican una mayor preocupación, ciertamente, pues la cantidad de tecnología y medios de comunicación, permiten situaciones inimaginables en la época de Warren y Brandeis como se pone en evidencia más adelante.

[76] PROSER, W. L., "Privacy", en *California Law Review*, vol. 48, No. 3, 1960, p. 107, [en línea], http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview

3.3. Inicios de la intimidad en Europa.

La trayectoria del derecho a la intimidad en Europa fue distinta de la de EE.UU. y tan sólo existieron formulaciones filosóficas y doctrinales sobre los derechos de la personalidad. En el seno del debate político y filosófico, podemos destacar las formulaciones de Benjamín Constant De Rebecque, Jeremy Bentham, Thomas Hobbes, John Looke, Robert Price y John Stuart Mill[77].

En Europa el derecho a la intimidad no aparece enunciado de forma expresa y como categoría independiente en los textos constitucionales hasta fechas, relativamente, recientes[78]. Este derecho fue teorizado como parte de los derechos de la personalidad. El primer texto constitucional en Europa que recogió de forma expresa el derecho a la intimidad fue la Constitución Portuguesa de 1976 en el artículo 26.1 y, posteriormente, lo hizo la Constitución Española[79] de 1978 en su artículo 18[80]. Ciertamente, en las codificaciones europeas se protegen el derecho

---

[77] PAREJO ALFONSO, L., "El derecho fundamental a la intimidad", *IUS ET PRAXIS*, Lima, *Revista de la Universidad de Lima,* No. 21-22, 1993, p. 40.

[78] El reconocimiento de la intimidad como derecho independiente se produce en una época relativamente reciente y así se manifiesta también en el ámbito de la legislación internacional que surge tras la Segunda Guerra Mundial.

[79] El Estatuto de Bayona, señalaba el domicilio como inviolable, sin embargo, no se reconoce expresamente hasta la Constitución de 1869 cuando la casa de habitación se reconoce como un derecho pleno para españoles y extranjeros, [en línea], http://webs.uvigo.es/mpsp/1808.htm

[80] En la Constitución Española el artículo 18.1 dispone que "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen". El artículo 18 acoge un contenido amplio de intimidad. Junto a la declaración general de positivación del derecho a la intimidad, se reconoce el derecho a la intimidad domiciliaria y a la libertad y confidencialidad de comunicaciones privadas, para acabar con la constitucionalización del "*habeas data*" o faceta informática de la intimidad que la "*privacy*" adopta frente a los peligros de la informática. El artículo 18.4 CE. reconoce la dimensión positiva de la intimidad convertida en "libertad informática", que básicamente constituye un derecho de control sobre los datos personales que circulan en la sociedad informatizada.

de intimidad de forma moderna atendiendo a las realidades contemporáneas propias de una sociedad electrónica.

Pareciera que el derecho a la intimidad se constituye en una garantía de la libertad personal, dado que si la información personal o familiar es distorsionada, se divulga sin responsabilidad o se produce una intromisión no consentida, ello ocasione un recorte o captura de la libertad, ya que tales actos no permiten que las personas adopten las decisiones de su existencia en forma libre y autónoma, sin estar afectado por la vulneración de su intimidad.[81]

La esfera privada pasa a convertirse de ese modo en un mundo de experiencia, de la conciencia, en el plano en donde se forman la escala de valores éticos del individuo y el hombre manifiesta su personalidad globalmente, formándose la esfera pública a partir de las relaciones entre particulares y expresa el marco abstracto e impersonal de la convivencia política en la sociedad de masas contemporánea postindustrial.[82]

El artículo 18.4 de la Constitución Española, establece que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Según PÉREZ LUÑO, esto supone un planteamiento fragmentario e individualista de la compleja serie de

---

[81] MIRANDA ALCÁNTARA, M. I., *Informática, intimidad y protección de Bases de datos* [en línea], http://www.teleley.com/articulos/art-miranda.pdf *v. et.* García San Miguel apunta que definamos como definamos la intimidad, casi todos admitirán que este derecho tiene que ver con la posibilidad de que algo de lo que hacemos o lo que somos (sean cuales sean los confines de ese *algo*) no sea conocido por los demás y, si fuera conocido por algunos, estos no lo den a conocer a otros. GARCÍA SAN MIGUEL RODRÍGUEZ-ARANGO, L., *Estudios sobre el Derecho a la Intimidad*, Editorial Tecnos S.A., Madrid, 1992. FALTA PÁGINA

[82] MORALES PRATS, F., *La tutela penal de la intimidad: privacy e informática,* Barcelona, 1984, p. 18.

cuestiones de matiz personal y social que hoy se debaten y suscitan en el marco de las relaciones entre intimidad e informática.[83] Conviene que se tenga presente, que tanto el artículo 18.4 como el artículo 105, *b)* remiten a una ley orgánica para delimitar el alcance y desarrollo de su contenido.

En la legislación Española[84] en materia de protección de datos, por ejemplo, se encuentran ambos términos en distintos textos legales. La Constitución Española[85] de 1978 solo utiliza el término *intimidad*, mientras que la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos (LORTAD)[86] introduce el término privacidad en 1992[87]. El Código Penal español, de 1995, define los delitos contra la intimidad (Título X)[88] y la Ley Orgánica de Protección de Datos de Carácter

---

[83] PÉREZ LUÑO, A. E., *op. cit., "La protección de la intimidad…".* p. 4.

[84] Legislación Española es tomada la Agencia Estatal Boletín Oficial del Estado del Ministerio de la Presidencia, consultable en, www.boe.es

[85] Ar. 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

[86] Normativa derogada. La referencia se tomó de la exposición de motivos de la LORTAD en la que se utilizó el término de privacidad.

[87] El término fue utilizado en la exposición de motivos (norma derogada).

[88] Art. 197. 1. El que, para descubrir los secretos o vulnerar la *intimidad* de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Personal de 1999 sostiene que su finalidad es proteger la intimidad personal y familiar[89].

Tal como ocurre en países europeos, debe evitarse la potencial agresividad de la información contra la intimidad de las personas, habida cuenta que resulta necesario protegerlas ante el manejo o manipulación, no autorizada, de sus datos personales, cuando estos son susceptibles de tratamiento informatizado.

Ante tal situación pareciera que no es suficiente el viejo hábeas corpus del ciudadano, que ve ante nuevas amenazas para su libertad y dignidad al perfeccionarse el poder de la tecnología informática, que no precisa constreñir la libertad y los derechos políticos, entre otros, por medio del control físico sobre el ciudadano, de ahí la importancia del derecho a la protección de datos.

Este poder informático constituye un nuevo modelo de información que sin vigilar a sujetos determinados, tiene como característica la posibilidad de intervenir en cualquier momento, de forma certera, cuando aparezca un peligro relevante para el sistema.[90]

Uno de los aspectos de mayor interés en la reglamentación jurídica de la informática a escala internacional es el que se refiere a la transmisión de datos personales entre diversos países. El problema del flujo transnacional o internacional

---

[89] Art. 1. Objeto. La presente Ley Orgánica tiene por objeto 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.

[90] FOUCAULT, M., "Nuevo orden interior y control social" en *El viejo topo*, No. 7; también en "Vigilar y castigar", 1era ed. - en francés -, París, 1975.

de datos (transborder data flow) ha suscitado un abierto conflicto de intereses entre los países productores y los países consumidores de datos informáticos. [91]

Los países tecnológicamente avanzados se hallan en condiciones de recoger informaciones, almacenarlas y distribuirlas con la utilización de la informática. Por el contrario, los países subdesarrollados sólo pueden recibir y consumir informaciones; es más, en determinados casos ni siquiera pueden servirse de ellas por carecer de los medios técnicos necesarios para aprovecharlas. Esta circunstancia ha determinado que los países desarrollados mantengan una posición decidida en favor de una libertad ilimitada de intercambios de informaciones entre todos los países; mientras que los países subdesarrollados, que carecen de una tecnología informática propia, exigen que se reconozca la facultad de ejercer un control sobre los datos que puedan recogerse en su territorio[92].

Además, los ciudadanos de los países desarrollados también son objeto de este proceso de vigilancia masiva, y constituyen sectores que sólo pueden recibir y consumir informaciones, sin que puedan generarlas, ya que la posibilidad de realizar almacenamientos masivos de información sensible se reduce a unas cuantas compañías privadas y al gobierno de algunos estados con alta capacidad tecnológica.

Una armonización legislativa internacional en los Estados Europeos sobre la protección de los datos personales sometidos a tratamiento informatizado por medios idóneos, constituía la aspiración capital del Convenio 108 del Consejo de Europa de 28 de enero de 1981. Esto es lo que se pretendió con el Convenio de

---

[91] *Vid.* BUSTAMANTE DONAS, J., "Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica", en *Revista Iberoamericana de Ciencia, tecnología, Sociedad e Innovación,* No. 1, Septiembre-Diciembre 2001, La Sociedad de la Información en Internet [en línea], http://www.campus-ei.org/revistactsi/numero1/bustamante.htm

[92] PEREZ LUÑO, A.E., *Derechos Humanos, Estado de Derecho y Constitución,* Editorial Tecnos S.A., Madrid, 5ª ed., 1995. FALTA PÁGINA

Estrasburgo, y en efecto se logró. El Convenio Europeo de 1981, como también se le conoce, relativo a la protección de personas en relación con el tratamiento automatizado de datos de carácter personal, fue ratificado por España el 27 de enero de 1984, con lo cual a partir de allí perteneció a los Estados con leyes de protección de datos de la segunda generación. Este texto, aparte de constituir norma jurídica de derecho interno en España, por el ingreso al ordenamiento jurídico (art.96.1 CE), es un eficaz instrumento de interpretación de los derechos humanos, en lo referente al uso de la informática.

El derecho de intimidad es inherente a la persona, que necesita de espacios libres de intromisiones en su vida individual y familiar, para lograr el pleno desarrollo de su personalidad y su identidad. Todos los seres humanos cuentan con una vida privada, conformada por aquella parte de la vida que no está consagrada a una actividad pública y que no trasciende a la sociedad de manera directa.

La protección del derecho a la intimidad en la legislación europea y americana se diferencia según se trate de autoridades públicas o privadas. En la legislación de Estados Unidos y Canadá, la protección de la intimidad en la esfera pública está garantizada como derecho constitucional de aplicación a las comunicaciones electrónicas y, por tanto, a Internet. Esta protección constitucional se aplica a los órganos gubernamentales.

De otra parte, en la legislación europea se contempla en cada uno de los ordenamientos de los países la protección desde las distintas Constituciones y las normas de desarrollo de estas dedicadas a la protección del derecho a la intimidad, junto con el Convenio Europeo de Derechos Humanos. Este Convenio limita las medidas adoptadas por las leyes nacionales de los Estados firmantes para permitir

el acceso a las comunicaciones en general, y las transmisiones en Internet en particular, por parte de las autoridades gubernamentales.[93]

También, en el ámbito europeo, encontramos en la legislación francesa, la protección de la confidencialidad de archivos y expedientes en Internet, la cual está garantizada por varias leyes. Así, la sección 25 de la Ley de 10 de julio de 1991[94] sobre confidencialidad de la correspondencia a través de servicios de telecomunicaciones, prevé sanciones contra cualquier operador público, de red o proveedor de servicio de telecomunicaciones que viole la confidencialidad de la correspondencia confiada al servicio en el que se participa, aun cuando el contenido de tal correspondencia no fuera divulgado ni usado, existiendo una excepción a favor de los proveedores de servicio de Internet (ISP), en caso de que su acto se justifique por necesidades técnicas.

En Internet, los proveedores de servicios, administradores de grupos de interés, y servidores Web, que mantienen archivos de datos personales están obligados a cumplir las reglas. En España la Ley 15/99 de protección de datos de carácter personal (LOPD)[95] que sustituyó a la LORTAD (Ley Orgánica para la Regulación del Tratamiento Automatizado de los Datos de Carácter Personal), exige la inscripción obligatoria de las bases de datos con información personal en el Registro de la Agencia Española de Protección de Datos[96]. Se requiere la autorización expresa de los titulares de la información, y los datos no se pueden

---

[93] FERNÁNDEZ ESTEBAN, M. L., "La regulación de la libertad de expresión en Internet, en Estados Unidos y en la Unión Europea", *Revista estudios políticos*, No. 103, 1999. FALTA PÁGINA

[94] CASTILLO JIMENES, C., *op. cit.,* p. 8.

[95] *Vid.* Ley Española, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, de 14-12-1999, pp. 43088-43099), [en línea], https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

[96] Agencia Española de Protección de Datos (AEPD) se puede consultar en: https://www.agpd.es

utilizar para una finalidad distinta a la que se haya autorizado, asimismo, no pueden transmitirse sin el consentimiento expreso de su titular.

La Agencia Española de Protección de Datos es un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, y que tiene por objeto la garantía del cumplimiento y aplicación de las previsiones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y sus normas de desarrollo.

El profesor Díaz Revorio señala al efecto que, a raíz de las tecnologías, se ha hecho necesario un concepto de intimidad más amplio, como lo sería el de vida privada o privacidad. A esta idea, hace referencia la exposición de motivos de la ya derogada LORTAD. En esta amplia dimensión de la vida privada se incluyen, aparte de la intimidad en sentido estricto, el secreto de las comunicaciones y la protección de datos personales, derechos que desde luego deben ser preservados ante las amenazas que Internet puede suponer para los mismos.[97]

Asimismo, también señala el citado autor, que la protección de la privacidad no ha de ampliarse sino también hacerse más intensa y rigurosa, buscando nuevos medios y elementos para impedir que la omnipresencia de la red llegue a convertirse en una especie de "gran hermano" que, acompañando a la persona en todo lugar, tiende a neutralizar cualquier dimensión de la vida privada.[98]

En el capítulo tercero *infra* se analizará el contenido actual del derecho de intimidad y los derechos que amplían su contenido, tales como: el derecho al honor, imagen, libertad informática, protección de datos personales, inviolabilidad de

---

[97] DÍAZ REVORIO, F.J., *Los derechos humanos ante los nuevos avances científicos y tecnológicos. Genética e internet ante la constitución,* Tirant Lo Blanch, Valencia, 2009, p.193.

[98] *Ibíd.*

domicilio y secreto de las comunicaciones. Sin embargo, con el propósito de evidenciar la influencia de las tecnologías electrónicas de información y comunicación en el contenido de este derecho, resulta necesario dedicar unos apartados al estudio del impacto tecnológico en los derechos de la sociedad electrónica, antes de dedicarse al desarrollo del contenido actual de este derecho.

Los derechos fundamentales se han tenido que adaptar ante una sociedad de cambios. La convergencia de tecnologías que han introducido medios de comunicación electrónicos ha creado la necesidad de reformar la legislación que antes era utilizada para el mundo analógico. Se reconoce a Internet como uno de los fenómenos sociales más importantes dado su éxito y penetración. De hecho, ha propiciado cambios en la política, la economía, la sociedad y, evidentemente ha tenido grandes repercusiones en el ámbito normativo. Esta herramienta ha potenciado las conductas de las personas, al permitir una difusión capaz de superar las barreras temporales y espaciales. Sin embargo, la herramienta ha potenciado las conductas buenas y malas, lo cual ha hecho que se planteen distintas soluciones a fin de proteger a la población y garantizar la permanencia de Internet.

4. DERECHOS DE LA SOCIEDAD DEL CONOCIMIENTO O LOS DERECHOS DE CUARTA GENERACIÓN.

Existen varios derechos derivados de los derechos de privacidad e intimidad, como el derecho de imagen, el honor, y la protección de datos, los que gozan de autonomía propia. Si bien el derecho a la intimidad ha sido derivado del reconocimiento a la libertad personal ubicado en la primera generación de derechos, fue hasta la tercera generación que, en *"respuesta al fenómeno de la denominada contaminación de las libertades (liberties pollution)"* [99], el derecho a la intimidad alcanzó mayor protección, lo que originó que se viera precisado a ampliar su contenido por medio del reconocimiento de nuevas vertientes, para ahora tener una ramificación de derechos que han sido incorporados en este. Recientemente, se habla de la protección de los datos genéticos.[100]

Pareciera tratarse de nuevos derechos[101], los de futuras generaciones, derivados de la revolución tecnológica de finales del siglo XX y principios del siglo XXI; a los que se denominan *derechos en la sociedad del conocimiento*, por el

[99] ARELLANO TOLEDO, W. y OCHOA VILLICAÑA, A.M., "Derechos de privacidad e información en la sociedad de la información y en el entorno TIC", IUS, *Revista del Instituto de Ciencias Jurídicas de Puebla*, No. 31, enero -junio 2013, p. 5. *Vid*. PÉREZ LUÑO, A. E., *La tercera generación de derechos,* Thomson, Navarra, 2006, p. 28-29.

[100] *Cfr.* DÍAZ REVORIO, F.J., *Los derechos humanos ante…, op. cit.* pp. 117-164.

[101] Algunos autores, señalan que no se trata de nuevos derechos fundamentales, sino que son los mismos derechos existentes aplicados a nuevas situaciones. *Cfr.* RIASCOS GÓMEZ, L. O., "El derecho a la intimidad, visión iusinformática y el delito de los datos personales", *Tesis Doctoral,* Universidad de Lleida, España, 1999, p. 244; *v. et.* DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho Informático*, Editorial Aranzadi, Madrid, 10a ed., 2008, pp. 21 y ss.

contexto histórico en el que se originan y la incidencia de las tecnologías de la información y comunicación.

La división generacional de los Derechos Humanos corresponde a criterios históricos y temáticos. Por tal razón, si se habla de un cambio social con el surgimiento de la sociedad de la información, los derechos humanos también se han transformado y ello justifica una nueva división histórica satisfaga el ámbito de explicación doctrinal que cubriría este nuevo compendio de derechos.

Efectivamente, estamos ante una nueva sociedad de cambios. En el ámbito político internacional, el orden cosmopolita al que alude Habermas en su obra, *La inclusión del otro*[102], ha logrado introducir innovaciones que obligan a las sociedades a adoptar nuevas medidas para la convivencia mundial a través incluso de la ampliación de los límites de la acción internacional. Los problemas del mundo ya no afectan a un sector de la sociedad, sino que afectan a todos, e incluso la amenaza de la guerra se ha globalizado.

En el plano de los derechos humanos, las Tecnologías de la Información y la Comunicación (TIC) han introducido amenazas comunes que obligan a la ampliación de la protección de los derechos del ser humano. La interacción entre la comunicación y la telemática en esta nueva era, ha posibilitado un mundo de información en tiempo real, de transmisión masiva y asimilación simultánea de esa información. Esta dinámica ha generado cambios en el plano jurídico, social y político que exigen respuestas universales y no aisladas. Efectivamente, la convergencia de tecnologías ha introducido medios de comunicación inéditos cuya implementación pone en jaque la aplicación de la legislación que antes era utilizada

---

[102] HABERMAS, J., *La inclusión del otro, estudios sobre teoría política*, Paidós, Barcelona, 1999, p. 23. *v. et.,* GIDDENS, A., *Consecuencias de la modernidad,* Alianza Universidad, Madrid, 1994, p. 28.

para el mundo analógico, en lo que respecta a la protección de derechos como la intimidad personal, la inviolabilidad de las comunicaciones y el derecho de la propiedad intelectual, entre otros.[103]

Los derechos de la cuarta generación constituyen una categoría que se distingue de los derechos de la tercera en función de su carácter formal o material. Ambas generaciones de derechos funcionan como principios ordenadores de la sociedad internacional, pero mientras los derechos de la tercera generación enfatizan la igualdad *formal* de los Estados, los de la cuarta generación apuntan a lograr una mayor igualdad *material* de oportunidades de desarrollo entre ellos. De este modo se establece entre las generaciones tercera y cuarta una relación de complementariedad (y en ocasiones de tensión), paralela al vínculo entre la primera y la segunda generaciones."[104]

---

[103] CASTRO BONILLA, A., "Los Derechos Fundamentales en Internet. Costa Rica", *Revista Electrónica de Derecho Informático,* No. 50, [en línea], http://www.hacienda.go.cr/centro/datos/Articulo/Los%20Derechos%20Fundamentales%20en%20Internet.doc

[104] FIX FIERRO, H., "El juicio de amparo mexicano y el recurso constitucional federal alemán", *Boletín Mexicano de Derecho Comparado*, Instituto de Investigaciones Jurídicas UNAM, No. 77, 1993, [en línea], http://biblio.juridicas.unam.mx/revista/DerechoComparado/numero/77/art/art3.htm

5. AVANCE TECNOLÓGICO Y LA AFECTACIÓN DE LOS DERECHOS HUMANOS.

Uno de los más poderosos resortes del creciente interés por el fenómeno cibernético nace de la honda incertidumbre con que el hombre promedio contempla la compleja estructura del ordenar y sus posibles repercusiones para la convivencia[105]. Es una incertidumbre que se manifiesta en múltiples aspectos de la cultura, y que compromete no sólo el futuro de esta nueva ciencia, sino la propia objetividad de nuestros criterios de valoración, generando, en ocasiones, un ansia hostil cuya sombra, en caso de propagarse, puede ser un freno insalvable para el progreso tecnológico[106].

Por lo anterior, es preciso que se establezcan una serie de medidas a fin de dotar a la sociedad, de una infraestructura que posibilite la institucionalización de auténticos controles del uso de la informática de índole técnica y jurídica, aunque existan dudas sobre la efectividad de los mismos. Es necesario, asimismo, coordinar eficazmente la legislación internacional y nacional relativa al uso de estas nuevas tecnologías.[107]

Uno de los aspectos interesantes de las nuevas tecnologías es la convergencia entre la tecnología de telecomunicaciones y la informática, es decir,

---

[105] Por la necesidad cada día mayor del derecho de regular materias del conocimiento humano, sobre todo las de índole tecnológico surgidas de la llamada informática, para que sean creadas, desarrolladas, protegidas, garantizadas y utilizadas conforme a un ordenamiento jurídico en vigor, es por lo que *Hernández Gil,* citado por *Davara,* comenta sobre los problemas socio-culturales de la informática jurídica, estima que el derecho *strictu sensu* no va a ordenar nuevas realidades, sino que el Derecho mismo va a experimentar, en cuanto objeto de conocimiento, una mutación, derivada de un modo distinto de ser elaborado, tratado y conocido. DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho Informático, op. cit.*, pp. 21 y ss.

[106] *Vid.* VILLATE, J., *La libertad de expresión en Internet: retos y amenazas* [en línea], http://www.une.edu.ve/~iramirez/te1/censura_internet.html

[107] *Cfr.* GOMEZ NAVAJAS, J., *op. cit.,* p. 38.

entre la telefonía, los nuevos servicios telemáticos (de telecomunicaciones e informática) y la radiodifusión (radio y televisión). Pronto no valdrá la pena distinguir entre un servicio u otro.

Las nuevas tecnologías marcan la vida diaria de las personas, en particular en el contexto de la globalización, de la cual pueden ser declaradas cómplices. En los últimos treinta años se viene registrando la aparición y difusión creciente de una serie de avances, nuevos conocimientos, formas de organización y procesos novedosos, fuentes de energía alternativas, etc., que permiten configurar un nuevo panorama marcado por el predominio de las tecnologías electrónicas. Estas tecnologías han dado un giro a las relaciones humanas dentro de la sociedad. Las relaciones entre la sociedad -o nosotros como sujetos individuales- y la tecnología son cada vez más evidentes[108].

Los medios actuales de comunicación modifican de forma radical el intercambio de información, que deja de ser dependiente del tipo de transporte, para

[108] La definición de la tecnología resulta especialmente difícil al ser indisociable de la propia definición del ser humano. Sin embargo, conviene tener en cuenta cuál es la idea más usual y tópica de esta. El DLE define la tecnología como el *"conjunto de los conocimientos propios de un oficio mecánico o arte industrial"*, o también como "*el conjunto de los instrumentos y procedimientos industriales de un determinado sector o producto"*. Sin embargo, en el contexto que se está utilizando este término, es necesario interpretarlo como una serie de sistemas diseñados para realizar alguna función. Se habla entonces de tecnología de sistemas y no sólo de artefactos, para incluir tanto instrumentos materiales como tecnologías de carácter organizativo (sistemas impositivos, de salud o educativos que puedan estar fundamentados en el conocimiento científico). La educación es un ejemplo claro de tecnología de organización social, así como los medios de comunicación, ya que la organización social resulta igualmente ser un artefacto relevante. Por tanto, lo tecnológico no es sólo lo que transforma y construye la realidad física, sino también aquello que transforma y construye la realidad social.

ser un proceso en el que la información se mueve a la velocidad de la luz. Las redes telemáticas de fibra óptica, permiten que mucha información que era previamente inaccesible y sin valor debido a que estaba en un lugar remoto, se convierta en útil y valioso a través de la red. Así, el acceso a bases de datos remotas y la transmisión de datos, sonidos e imágenes en tiempo real a cualquier parte del planeta son parte de la cotidianidad. Del mismo modo, personas con las cuales se podía mantener una relación a distancia puede ser ahora un compañero de trabajo que interactúa de un modo eficaz.

El problema crucial que plantea la sociedad de la información en el ámbito de los derechos, es el relativo a la desintegración social y la oposición de los que tienen acceso a las nuevas tecnologías y los que no pueden acceder a estas.[109]

En el futuro podrían existir diferentes modelos de sociedad de sociedad tecnológica, como ahora existen diferentes modelos de sociedades industrializadas. Es posible que difieran en el grado en el que evitan la exclusión social y en la creación de nuevas oportunidades para los menos afortunados. Por ello, la obligación de los poderes públicos de promover la igualdad y facilitar la participación de todos los ciudadanos en la vida pública adquiere así una nueva dimensión en la sociedad de la información.[110]

---

[109] Yoneji Masuda, estimó la sociedad de la información como uno de los sectores más importantes de la industria, "*la era de la información es el periodo durante el cual tiene lugar una innovación, se convierte en la fuerza latente de la transformación social, capaz de acarrear una expansión en la calidad y en la cantidad de información y un aumento en gran escala del almacenamiento de la información",* MASUDA, Y., *La sociedad informatizada como sociedad pos-industrial,* Fundescos Tecnos, Madrid, 1984, p. 20.

[110] Existe duda sobre quien acuño, por primera, vez el concepto de la sociedad tecnológica, entre los autores que se citan, están los trabajos de MACHLUP, F., *The production and distribution of knowledge in the United States,* Princeton University, New Jersey, 1971.; BELL, D., *El advenimiento de la sociedad post-industrial: un intento de prognosis social,* Alianza, Madrid, 1976; PORAT, M., *The information economy: definition and measurement*, Department of Commerce, United States, 1977; y, MASUDA, Y., *op. cit*. en 1984.

La difusión de las nuevas tecnologías aporta nuevas oportunidades para construir una sociedad más igualitaria y participativa. Evitar la exclusión de parte de la población constituye el reto más importante que plantea la era del conocimiento. Uno de los principales riesgos de la sociedad tecnológica reside en la creación de una "sociedad de dos velocidades", en la que una parte de la población tenga acceso a la tecnología, la maneje con soltura y goce plenamente de sus beneficios, mientras que otra parte quede absolutamente excluida, fenómeno que es definido como *brecha digital*.

Lo anterior plantea la necesidad de establecer salvaguardas jurídicas y de garantizar la cohesión de la nueva sociedad. Deberá garantizarse a todos unos accesos equitativos a la infraestructura, al igual que la prestación de un servicio universal, cuya definición debe ir de la mano de la evolución tecnológica. La educación, la formación y la promoción desempeñarán necesariamente un papel fundamental.[111]

Por otra parte, los cambios en la tecnología son más relevantes que nunca para el mundo jurídico. Entre los juristas se observa una cierta reticencia a considerar las nuevas tecnologías como algo que va a condicionar el modo en el que entendemos la realidad, y por tanto, el modo en que el Derecho debe hacerle frente.[112]

---

[111] ORTEGA MARTÍNEZ, J., *Sociedad de la información y derechos humanos de cuarta generación. Un desafío inmediato para el derecho constitucional,* Derecho Constitucional, Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados, [en línea], http://www.bibliojuridica.org/libros/libro.htm?l=1510

[112] Estudillo señala que *"El cambio tecnológico ha alterado profundamente la naturaleza y el carácter central de la actividad industrial en la sociedad. El crecimiento de la industria y los servicios no es ya el ímpetu principal del desarrollo social, y además, está siendo reemplazado por una fuerza todavía*

Entender la tecnología y las posibilidades que ofrece, aunque sea de un modo profano, es la clave para comprender el modo en que ésta va a determinar el ejercicio futuro de los derechos y a alterar concepciones jurídicas pensadas para el mundo real. Así, la noción de escasez en la utilización de las *ondas hertzianas*[113], ha permitido y justificado la intervención, e incluso la censura indirecta en las cadenas de televisión, carece de sentido con las posibilidades que ofrece la fibra óptica y la transmisión digital.

En lo que respecta al Derecho Constitucional, las nuevas tecnologías e Internet plantean uno de los desafíos más interesantes de los últimos tiempos. Algunos casos aparecidos en la prensa, como la publicación en Internet del libro del Dr. C. Gubber y Mr. Gonod (titulado "Le grand secret") sobre el historial médico de Francois Mitterrand, información que había sido secuestrada judicialmente, ponen de manifiesto, por un lado, la insuficiencia de los instrumentos jurídicos pensados para proteger al individuo en el mundo real, y por otro, la agresividad del nuevo medio. Los derechos fundamentales más afectados por las nuevas tecnologías a primera vista son los derechos a una comunicación libre y los derechos fundamentales relativos a la vida privada.

Sin negar la evidencia de la evolución del Derecho y de nuevas categorías inexistentes en épocas anteriores, lo cierto es que las categorías actualmente existentes nos permiten afrontar con relativo éxito los retos que plantean las nuevas técnicas. Esto no excluye que tales desafíos puedan ser superados mediante la

---

no definida, basada en la información". ESTUDILLO GARCÍA, J., "Surgimiento de la sociedad de la información", Biblioteca Universidad, *Nueva Época*, vol. 4, No. 2, julio-diciembre 2001, p. 77.

[113] Onda electromagnética que se propaga por el espacio sin guía artificial y cuya frecuencia es convencionalmente inferior a 3 000 GHz.

construcción de nuevas “reglas” que prescriban determinadas conductas sin más excepciones que las expresamente previstas por la norma[114].

Como afirma Graciano González[115], una consideración filosófica de los valores de razón, dignidad, libertad, igualdad, solidaridad y paz, que expresan dicha condición, debe realizarse a través de un discurso que considere los derechos humanos como exigencias morales de realización, tanto en el nivel personal como en el comunitario. Introducir la tecnología en este contexto significa atender a la necesidad de traducir dicho discurso en términos que puedan también abarcar a la ciencia y a la tecnología como elementos que modifican el concepto de espacio o ámbito en el que se manifiestan, profundizan, y desarrollan los derechos humanos.

Por su parte, señala Ignacio Ramonet[116], el ciberespacio está siendo colonizado despiadadamente por todos los gigantes de las telecomunicaciones. Internet está creando nuevas formas de desigualdad entre “inforricos” e “infopobres”, al establecer discriminaciones graves en el acceso y utilización de informaciones entre el Norte y el Sur, donde la falta de equipos va a condenar a la marginación a millones de personas. Recuerda, por ejemplo, que hay más líneas telefónicas sólo en la isla de Manhattan (Nueva York) que, en toda África, y sin esas líneas no se puede acceder a Internet.

Según Ramonet resulta ingenuo pensar que, necesariamente, el aumento de comunicación debe traducirse en mayor equilibrio y armonía social. La

---

[114] *Vid.* RUIZ MUGUEL, C., *op. cit.,* p. 50-56.

[115] GONZÁLEZ, G., *Derechos Humanos: La condición humana en la sociedad tecnológica,* Tecnos, Madrid, 1999, p. 233.

[116] RAMONET, I., citado por PEREZ LUÑO, A. E., *Internet y los derechos humanos* [en línea], http://www.uhu.es/derechoyconocimiento/DyC02/DYC002_A05.pdf

comunicación, en sí, no es progreso social *"y mucho menos cuando la controla, como es el caso de Internet, las grandes firmas comerciales y cuando, por otra parte, contribuye a acrecentar las diferencias y desigualdades entre ciudadanos de un mismo país, y habitantes de un mismo planeta*".[117]

La naturaleza multidisciplinaria de los derechos humanos (ética, jurídica, antropológica, política, tecnológica, etc.) les permite ocupar un papel central en esos debates y estudios. La libertad de expresión no es sólo uno de los derechos humanos fundamentales, sino también una de las condiciones necesarias para el desarrollo de los demás derechos. Sin él, la vida humana pierde una de sus características más sustantivas[118]. Entre los derechos contenidos en la Declaración Universal de los Derechos Humanos de 1948[119] cobra un papel fundamental el reconocimiento de: a) la libertad de pensamiento, de conciencia y de religión (artículo 18); b) la libertad de investigar y recibir información (artículo 19) y; c) la libertad de opinión y de difundirla sin limitación de fronteras, por cualquier medio de expresión (artículo 19).

Por el hecho de ser Internet una infraestructura técnica orientada a proporcionar una cobertura de comunicación barata, horizontal y de ámbito global, estas libertades no sólo deben aplicarse en toda su extensión a las actividades personales que se llevan a cabo en la red, sino que cobran aquí una relevancia que no aparece en los medios tradicionales de comunicación. Teóricamente cualquier persona puede exponer sus opiniones a través de estos medios. En la práctica, sólo los grandes grupos de la comunicación y aquellos que componen los variados

---

[117] *Ibíd.*

[118] BUSTAMANTE DONAS, J., "Derechos Humanos en el ciberespacio", en GONZÁLEZ, Graciano, *Derechos Humanos: La condición humana en la sociedad tecnológica,* Tecnos, Madrid, 1999, p. 164.

[119] *Declaración Universal de los Derechos Humanos de 1948*, [en línea], http://www.un.org/spanish/aboutun/hrights.htm

mecanismos del poder social tienen la posibilidad real de hacer oír su voz cuando pretenden utilizar los medios tradicionales como la radio, la televisión o la prensa. Por el contrario, en Internet muy pocos medios son suficientes para comunicar un mensaje, y para hacerlo llegar a todos los rincones del globo.

Internet es considerado un instrumento y el empleo de este se da para lo mejor y lo peor. A finales del año 2010 y principios del año 2011 los términos de revolución se pusieron de moda en Facebook y Twitter, movimientos online se combinaban con manifestaciones de personas para precipitar la caída de dictadores en Túnez y Egipto. Las redes sociales funcionaron como cajas de resonancia, transmitiendo y evidenciando las manifestaciones y revueltas árabes pese a la censura de la prensa oficial[120].

Cualquiera puede crear sus páginas web, participar activamente en foros de discusión, enviar y recibir mensajes de correo electrónico a un coste prácticamente nulo.

En la red, cualquier ciudadano se convierte en emisor y receptor a un tiempo, y la interactividad y la participación se revelan como regla básica del juego. Todas estas características son ajenas a los medios tradicionales. Sin una pluralidad de

---

[120] SOENGAS-PÉREZ, X., "El papel de Internet y de las redes sociales en las revueltas árabes: una alternativa a la censura de la prensa oficial" en Revista *Comunicar 41: Los agujeros negros de la comunicación,* vol. 21 - 2013, [en línea], http://www.revistacomunicar.com/indice/articulo.php?numero=41-2013-14. Un estudio detallado sobre el papel de Internet en la *primavera árabe* es desarrollado por este autor, en el cual se evidencia el cual los ciudadanos estaban intercomunicados e informados en todo momento, tanto internamente como con el exterior, prácticamente gratis y con feed-back casi inmediato. Gracias a estas posibilidades se desarrolló un fenómeno comunicativo sin precedentes que facilitaba la comunicación y la relación virtual entre personas con perfiles muy diferentes, un intercambio comunicativo plural, pero con un objetivo común: el interés por la evolución de los conflictos sociales y políticos surgidos en varios países árabes. Considera que estos servicios (redes sociales) fueron los responsables de parte del éxito (o del protagonismo) de la Red en las revueltas árabes porque, aunque no existía una coordinación profesional entre los activistas, el hecho de posibilitar el contacto entre los ciudadanos permitió mejorar las condiciones para organizar acciones conjuntas, algo esencial en la programación y en el desarrollo de las protestas.

fuentes no se puede hablar de libertad de pensamiento, conciencia o religión. Sin acceso a los medios de alcance internacional no tiene sentido hablar de libertad de opinión y de difusión de las mismas sin limitación de fronteras.

Estas características tienen un doble origen. Por una parte, la naturaleza de la digitalización, que homogeniza todo tipo de datos e información, ya sea audiovisual, textual o de cualquier otro tipo, y el progresivo desarrollo y abaratamiento de las tecnologías de la información y comunicación, hacen que su uso se extienda cada vez más y sea más difícil de restringir su disfrute a sectores habitualmente desfavorecidos de la sociedad. Por otra parte, la red tiene un diseño y una estructura que responden a una voluntad consciente orientada a la promoción de un medio democrático de libre expresión, voluntad que ha caracterizado la acción de muchas personas que han intervenido su desarrollo y en la progresiva expansión de sus aplicaciones. Ya se habla de una Internet 2 (I2) ó UCAID (*University Corporation for Advanced Internet Development*)[121], y no parece casualidad. Por lo anteriormente expuesto, la red es un escaparate de ideas, un foro de expresión universal, que atenta contra la inercia controladora de los Estados frente a los individuos. Parece pues, más sencillo crear una nueva red con un diseño realizado bajo parámetros de interés corporativo y gubernamental, en lugar de intentar controlar y censurar un espacio en el que la libertad de expresión se ha convertido en norma cotidiana.

Como conclusión, se podría afirmar que el desarrollo social y moral del ser humano no ha sido nunca opuesto al desarrollo de las realidades técnicas

[121] Es una red telemática de aplicaciones y tecnologías avanzadas, la mayoría para transferir información a alta velocidad, desarrollada principalmente por las universidades estadounidenses, construida en fibra óptica y permite altas velocidades con una gran fiabilidad. Es llevada por 212 universidades de Estados Unidos y otras 60 compañías tecnológicas como Comcast, Microsoft, Intel, Sun Microsystems y Cisco Systems. Algunas de las tecnologías que han desarrollado han sido IPv6, IP Multicast y Calidad de Servicio (QoS). Al respecto, puede consultarse en: http://www.internet2.edu/

científicas, pues dichas realidades se constituyen en condición de posibilidad para el cambio social, la emergencia de nuevos valores, la aparición de nuevos paradigmas éticos y, en definitiva, el advenimiento de nuevas formas de organización social.

Para describir la sociedad de la información se han utilizados sistemas socioeconómicos que emplean extensivamente la información en las áreas de su actividad.

Es por esa razón que resulta necesario que se reflexione constantemente y sobre el sentido de la relación entre los desarrollos técnicos y el entorno humano. Resulta evidente constatar que la tecnociencia está presente como uno de los hechos configuradores de la realidad actual, y que el mundo ha cambiado de forma sustancial a partir de ese impulso. Pero también debemos entenderlo como un fenómeno multidimensional que proyecta su influencia de una manera directa sobre las realidades morales, psicológicas y sociales.

El *derecho de intimidad* ha venido evolucionando conforme se desarrollan nuevas tecnologías, perfilándose una nueva concepción; supone, este derecho, un presupuesto para el ejercicio de otros derechos también fundamentales, como: la libertad de pensamiento, libertad de culto y un conjunto de derechos sociales, entre ellos la salud, costumbres, hábitos sexuales, ideas políticas, fe religiosa y aspectos sociales y económicos (todos considerados datos sensibles). Lo anterior evidencia el cambio en el contenido del concepto de intimidad a causa del desarrollo tecnológico de los sistemas informáticos.

Anteriormente, el derecho a la intimidad se definía como el derecho a ser dejado a solas o a la no intromisión en los asuntos personales o familiares de un individuo sin su autorización; ahora se concibe como el derecho del individuo a decidir si desea compartir sus pensamientos, sentimientos y los hechos de su vida personal o familiar por el acceso no autorizado a bases de datos que contengan información reservada.

Esta situación ha generado el surgimiento de un nuevo derecho, *la libertad informática,* que implica tanto el derecho del individuo a negarse a brindar información sobre sí mismo y el derecho a pretender información referida a su persona o personalidad; en suma controlar la identidad personal informática a través del consentimiento para preservar, acceder, o rectificar datos informativos referidos a la vida privada de las persona.[122]

El desarrollo de la informática crea una auténtica revolución en el ámbito de los métodos tradicionales para la organización, registro y utilización de informaciones. La dimensión cuantitativa de las informaciones, almacenadas y transmitidas, es de tal magnitud, que ha dado lugar a un auténtico cambio cualitativo, obligando a considerar el problema de las relaciones entre intimidad e información bajo un nuevo prisma.[123]

La necesidad de tutelar la vida privada de los individuos ha rebasado, en los últimos años, la esfera estricta del derecho interno para plantearse como una exigencia del orden jurídico internacional. Veinte años después de que se hubiera promulgado la Declaración Universal de los Derechos Humanos, la Asamblea General de la ONU, en su sesión del 19 de diciembre de 1968, adoptó una Resolución referente a los Derechos del hombre y progresos de la ciencia y de la

---

[122] *Vid.* Davara Rodríguez quien define privacidad como término al que podemos hacer referencia bajo la óptica de la pertenencia de los datos a una persona -su titular- y que en ellos se pueden analizar aspectos que individualmente no tienen mayor trascendencia, pero que al unirlos a otros pueden configurar un perfil determinado sobre una o varias características del individuo, que este tiene derecho a exigir que permanezcan en su esfera interna, en su ámbito de privacidad. DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho Informático, op. cit.*, p. 55.

[123] PÉREZ LUÑO, A. E., "La protección de la intimidad frente a la informática en la Constitución Española de 1978"*. Derechos económicos, sociales y culturales : para una integración histórica y doctrinal de los derechos humanos: actas de las IV Jornadas de Profesores de Filosofía del Derecho*, Murcia, 1981, [en línea], http://www.cepc.es/rap/Publicaciones/Revistas/3/REPNE_009_059.pdf

técnica. En dicha Resolución se instaba al Secretario General a impulsar, con la ayuda de las pertinentes comisiones consultivas, el estudio de los problemas planteados por el desarrollo científico y tecnológico en relación con los derechos del hombre y, en particular: a) la protección de los individuos y de las naciones frente al progreso de las técnicas de registro y comunicación de datos; b) las utilizaciones de la electrónica que pueden interferir el ejercicio de los derechos fundamentales en una sociedad democrática; y c) la búsqueda de un equilibrio entre el progreso científico y técnico y el desarrollo social, cultural y moral de la humanidad[124].

[124] Resolución de la Asamblea General de la ONU No. 2.450 de 19 de diciembre de 1968 sobre "Derechos del hombre y progresos de la ciencia y de la técnica".

CAPÍTULO III. NATURALEZA JURÍDICA Y CONTENIDO DEL DERECHO DE INTIMIDAD.

"La apertura es la desnudez de una piel expuesta a la herida y al ultraje. La apertura es la vulnerabilidad de una piel que se ofrece, ultrajada y herida, más allá de todo lo que se puede mostrar, más allá de todo lo que de la esencia del ser puede exponerse a la comprensión y a la celebración".[125]

[125] LEVINAS, E., *Humanismo del otro hombre,* Siglo XXI, 6ª ed., México-Madrid, 2006, p. 121.

1. CONSIDERACIONES PRELIMINARES.

El derecho de intimidad es un derecho fundamental ubicado por gran parte de la doctrina entre los derechos personales[126] y, por su desarrollo histórico, se le cataloga entre los derechos de fundamentales de primera generación. Con el paso del tiempo este derecho ha ampliado su ámbito de protección, proyectándose como el derecho al honor, derecho de imagen, la inviolabilidad de domicilio y comunicaciones y la protección de los datos personales.

Es un derecho fundamental porque, es indispensable para que una persona se pueda desarrollar, sin obstáculos ni interferencias, en una vida plena y digna, por esa razón el derecho de intimidad es un derecho subjetivo[127].

Para revelar el verdadero contenido de un derecho fundamental resulta práctico el estudio de su naturaleza jurídica, así como el estudio de los intereses jurídicos protegidos.

---

[126] Para Luciano Parejo, la intimidad hace referencia a un espacio propio, privativo del individuo, solo adquiere su propio sentido frente a los otros, tanto para hacerlo valer ante y contra, oponerlos a estos; como para compartirlos con ellos. PAREJO L., *El Derecho Fundamental a la intimidad. Problemas Actuales de los Derechos Fundamentales,* Madrid, España, 1994, p 294; Para, Pierini la intimidad es el poder o potestad de tener un domicilio particular, papeles privados, ejercer actividades, tener contactos y pensamientos que no trascienden a terceros, en virtud del interés personal de mantenerlos en reserva y la discreción de quien se entera de hacerlos públicos cuando se trata de hechos privados o datos sensibles de las personas. PIERINI A*., Hábeas data: derecho a la intimidad*, Universidad, Buenos Aires, 2002, p. 219.

[127] El derecho a la intimidad además de un derecho subjetivo, es un derecho positivo y esencial en la organización social, una garantía institucional de pluralismo y democracia, puesto que si lo público está regido por la pretensión de igualdad, lo privado es el origen de la singularidad; el respeto a la diferencia implica originariamente respeto a la vida privada y por tanto puede considerarse como una expresión o manifestación de libertad, así como una consecuencia de la dignidad humana en su condición de fundamento del orden político y de la paz social, *vid.* REBOLLO DELGADO, L., *op. cit.*, p. 118 y ss.

Las ideas básicas sobre la naturaleza jurídica del derecho a la intimidad se vinculan con las diversas apreciaciones relacionadas con el concepto. Se debe considerar con especial atención la evolución doctrinal, normativa y jurisprudencial de este derecho, pues pareciera distinto, dependiente del país y su área de influencia, provocando que su contenido varíe de forma sustancial en función del ordenamiento jurídico que se trate.

Anita Allen, cuando se refiere a las nociones cotidianas de la privacidad, estima se puede desdoblar el concepto para dividirle en privacidad *física*, que se refiere a la también llamada "espacial" que está delimitada por el espacio íntimo de una persona y la privacidad *informativa*, relacionada con los datos secretos o confidenciales de las personas. También se refiere a la privacidad de *locación* como un híbrido: la privacidad de la información física, es decir, la geográfica o paradero de una persona[128].

Según Sagardoy Bengoechea, "*el derecho a la intimidad es proteiforme, pues tiene muy variadas manifestaciones, todas ellas ligadas a la dignidad humana…"*[129], que comprende los siguientes campos: intimidad personal corporal o física; intimidad personal psíquica; intimidad personal económica; intimidad personal social y profesional; intimidad personal informática; intimidad personal ideológica y religiosa; intimidad personal sexual y de hábitos o costumbres; intimidad personal de la comunicación con otras personas; e intimidad personal sindical.

El derecho de intimidad podría entenderse como un derecho personal, que se adquiere por la consideración de la condición humana. Las tecnologías de información y comunicación han provocado que este derecho, así como los

---

[128] ALLEN, ANITA L., *Unpopular Privacy: What must we hide?,* Oxfort University Press, New York, 2011, [versión para lector digital Kindle].

[129] SAGARDOY BENGOECHEA, J. A., *Los derechos fundamentales y contrato de trabajo,* Civitas, Madrid, 2005, p. 56.

derechos que se manifiestan a través de este, están en constante revisión para ajustarse a los cambios propios de una sociedad tecnológica que plantea grandes desafíos para en cuanto a la protección jurídica de derecho que fueron concebidos en una sociedad analógica, con excepción del derecho a la protección de los datos de las personas.

Algunos autores consideran que los orígenes jurídicos del derecho de intimidad se remontan al derecho anglosajón[130], sin embargo, existen otros que estiman que ese derecho se asocia a dos vertientes previas como valor: el cristianismo y su modalidad reformista a finales de la edad media, ligada a la desaparición de la sociedad feudal y, de otra parte, con la Revolución Francesa y el eventual surgimiento de la burguesía capitalista, quienes tenían la posibilidad económica y social de apartarse de la sociedad.

Una de las teorías que explica el derecho a la intimidad fue la desarrollada por el Tribunal Constitucional Alemán, a través de la teoría de las esferas, que se basa en una concepción tradicional del derecho a la intimidad y distingue tres esferas o círculos concéntricos de lo individual, lo privado y lo íntimo. Ante esta teoría se presenta otra, llamada teoría del mosaico, la cual explica que, los datos aislados forman en su conjunto un determinado significado, mientras que por separado carecen de este.

[130] Existe casi unanimidad en la doctrina al aceptar la obra de Warren y Brandeis "The right to privacy" como el origen jurídico del término de privacidad. WARREN S. D., y BRANDEIS, L. D., "The Right to Privacy", *op. cit.*, [en línea], http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Otra de las teorías del derecho de intimidad es la anglosajona, *right to privacy,* desarrollada en el año 1960 por William Prosser[131], quien divide el concepto unitario de privacidad, en cuatro situaciones distintas de violación: la intrusión, la apropiación, la divulgación y la falsa luz[132], conocidos como leyes de responsabilidad civil (*torts law*).

[131] PROSER, W. L., "Privacy", *California Law Review,* vol. 48, No. 3, 1960, p. 389, [en línea], http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview

[132] Vid. *Infra* Capítulo III, apartado 2.1.4.

2. DERECHO DE INTIMIDAD.

En el capítulo II, en el apartado 3.2 *supra,* se anotaron algunas referencias del origen del derecho de intimidad. Se adelanta que el contenido de esta protección de derecho ha aumentado y de este se desprenden derechos que, hoy día, podrían estimarse como autónomos como: el derecho de intimidad, al honor, a la inviolabilidad de la propiedad y las comunicaciones y la protección de datos, presentándose este último como el más reciente.

La doctrina española[133] ha admitido que los derechos de la personalidad se adquieren con la consideración de la condición humana en el desarrollo del ordenamiento jurídico. Esos derechos nacen con la persona y se convierten por el ordenamiento en un valor jurídico tutelado.

Se ha mencionado que la intimidad como concepto jurídico fue desarrollado en EE.UU. como el derecho de estar solo *"the right to be alone"* en 1873.[134] Posteriormente, en 1890, Warren y Brandeis publicaron "*The right to privacy",* en el que desarrollaron el concepto jurídico de *privacy,* configurándola como un derecho a la soledad, como la facultad "*to be let alone*".[135] De ahí que la frase inglesa *my*

---

[133] HERRÁN ORTÍZ, A. I., *El derecho a la intimidad en la nueva Ley Orgánica de Protección de datos personales,* Ed. Dykinson, Madrid, 2003, pp. 2 y ss.

[134] En 1873, el Juez Thomas McIntyre Cooley, en su obra *"The Elements of Torts",* lo definió como *"the right to be let alone"*, es decir, el derecho a ser dejado en paz, o a ser dejado sólo. COOLEY, T. M., *The elements of torts, Callaghan and Company*, 1895, *op. cit., s.n.*

[135] WARREN S. D. y BRANDEIS L. D., *The Right to Privacy, op. cit.;* Se debe aclarar que ni la Constitución norteamericana de 1787 ni sus enmiendas reconocen, expresamente, el derecho a la privacidad, por lo menos como *right to privacy*. Este derecho ha sido reconocido en la jurisprudencia del Tribunal Supremo y se desprende de otros derechos reconocidos, como en el caso de la primera enmienda del derecho de asociación y en el caso de la cuarta enmienda frente a los registros personales y domiciliarios.

home is my castle (mi casa es mi castillo) reflejaba el espíritu de lo que se intentaba proteger. Podría estimarse que este derecho no surge como una exigencia natural del ser humano sino como el privilegio de una clase.

Con respecto a si el concepto de intimidad es sinónimo de privacidad, el autor comparte la tesis de Díaz Rojo, que al respecto concluye que *lo íntimo es privado pero no todo los privado es íntimo*[136]*.* Dado que semánticamente, ambos conceptos resultan tener un contenido distinto.[137]

Tal y como se había indicado, desde la tesis iusnaturalistas se explica el paso de los derechos personales a los derechos fundamentales como la materialización del valor de la dignidad humana. De otra parte, la tesis positivista no concibe reconocer derechos fundamentales que no se hallen, expresamente, consagrados en una Carta constitucional. En ese sentido una tesis iusnaturalista moderna se empeña en estimar los derechos fundamentales como la respuesta de los intereses sociales de cada momento histórico, los que son necesarios para el desarrollo pleno de las personas y que deben ser captados a través de una interpretación progresiva de la Constitución.[138]

Este derecho ha evolucionado y ha perdido la connotación negativa que le dio origen, la cual era entendida como el derecho a ser dejado a solas. Esta connotación particular del derecho solo permitía la defensa de este frente a otras personas. La evolución del derecho lo ha convertido en un derecho de connotación positiva, mediante el cual las personas tienen el derecho a disponer sobre los

---

[136] DÍAZ ROJO, J. A., *op. cit.,* [en línea].

[137] En ese sentido se puede consultar en el Capítulo II, apartado 2 *supra,* consideraciones terminológicas del concepto de privacidad e intimidad.

[138] *Cfr.* PÉREZ LUÑO, A. E., Derechos *Humanos, Estado de Derecho… op. cit.,* pp. 325-326.

aspectos de su vida que desean compartir con otras personas, tales como sus pensamientos, sentimientos y los hechos de su vida personal o familiar.

Positivar el derecho de intimidad y el reconocimiento jurisprudencial refleja la necesidad de protección de las interferencias de terceros en la vida privada de las personas. Se estima que el hecho de que su contenido sea ampliado denota la transición a una sociedad tecnológicamente evolucionada.

Este derecho ha sido reconocido por parte del Derecho Internacional de los Derechos Humanos, colocándolo en una posición de derecho universal, de rango superior. Este derecho ha sido reconocido en la mayoría de ordenamientos jurídicos nacionales como un derecho constitucional, al menos en América y Europa.

La Declaración Americana de Derechos y Deberes del Hombre, de 2 de mayo de 1948[139], es el primer texto que reconoce el derecho de intimidad y en el art. 5 establece que toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

Solo unos meses después, el 10 de diciembre de 1948[140], la Declaración Universal de los Derechos Humanos señala en su art. 12 que "*nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene el derecho a la protección de la ley contra tales ataques o injerencias*", reconociendo con carácter universal este derecho.

---

[139] *Declaración Americana de Derechos y Deberes del Hombre de 2 de mayo de 1948*. Artículo V, [en línea], http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

[140] *Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948*. Artículo 12 [en línea], http://www.un.org/es/documents/udhr/

También se reconoce este derecho en el artículo 8.1 de la Convención Europea para la protección de los Derechos Humanos y de las Libertades fundamentales de 1950[141], en el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos de 1966[142] y, por último, se reconoce el derecho a la protección de la intimidad en el Pacto de San José de Costa Rica de 1970[143], en el artículo 11.

Para Miguel Ekmekdjian y Calogeno Pizzolo el derecho a la intimidad *"es el derecho que tiene cada persona de disponer de una esfera, espacio privativo o reducto inderogable de libertad individual, el cual no puede ser invadido por terceros, ya sean particulares o el propio Estado, mediante intromisiones que pueden asumir muy diversos signos"*[144].

De otra parte, Castán Tobeñas[145] estima que los derechos son distintos de la personalidad misma, se refiere a una abstracta posibilidad de la cual está investida la persona, en tanto que los derechos de la personalidad no lo son todos los atribuibles a la persona, sino los que constituyen el núcleo esencial, por lo que

---

[141] *Convención Europea para la protección de los Derechos Humanos y de las libertades fundamentales.* Art. 8.1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia, [en línea], http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/SpanishEspagnol.pdf

[142] *Pacto Internacional de Derechos Civiles y Políticos.* Art. 17.1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación, [en línea], http://www.unhchr.ch/spanish/html/menu3/b/a_ccpr_sp.htm

[143] *Pacto de San José.* Art. 11. 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. 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. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. [en línea], http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

[144] EKMEKDJIAN, M. Á. y PIZZOLO, C., *Hábeas Data. El derecho a la intimidad frente a la revolución informática*, Ediciones Depalma, Buenos Aires, 1996, p 7.

[145] CASTAN TOBEÑAS, J., "Los derechos de la personalidad", *Revista General de Legislación y Jurisprudencia,* núm. 1-2, 1952, pp. 5-55.

propone las denominaciones de derechos esenciales de la persona o derechos subjetivos esenciales, porque se subraya así el carácter restringido y la importancia de estos derechos vinculados a la idea y esencia misma de la personalidad y naturaleza humana. Concluye reconociendo que el objeto de los derechos de la personalidad no se encuentra ni en la persona misma, ni en los obligados a su respeto, sino en los bienes constituidos por determinados atributos o cualidades físicas o morales del hombre, individualizadas por el ordenamiento.

Pareciera que se introduce un concepto restringido y limitado de los derechos de la personalidad, pues no todos los derechos de la persona vinculados al individuo, ostentan la consideración de derechos de la personalidad, sólo aquellos que identifican y califican a la persona, los que constituyen el núcleo esencial de la misma, entre los cuales incluye los derechos que se refieren al respeto y reserva de la vida privada y de la individualidad de cada ser humano.

En España, la protección de estos derechos se encuentra amparada en la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, donde el legislador español desarrolla la disposición constitucional recogida en el artículo 18.1 CE.

El derecho a la intimidad está protegido en los instrumentos internacionales de derechos humanos, la mayoría de las constituciones y en la normativa ordinaria, que incluye, en algunos de los casos, la protección de la normativa penal.

2.1. Protección Convencional y Constitucional.

En este apartado se desarrolla, de forma muy general, la protección convencional del Derecho de intimidad y su tratamiento jurisprudencial en España, Estados Unidos y Costa Rica.

2.1.1. La protección convencional.

La doctrina que desarrolla el concepto *derecho de intimidad* reconoce que no existe uniformidad en el contenido. Concuerdan en que se ha ampliado de forma progresiva el conjunto de intereses relevantes que integran este derecho desde el ámbito constitucional.[146]

En los últimos años la tutela de la intimidad en el derecho interno se ha planteado como una exigencia de orden jurídico mundial. En ese sentido, los tratados de derechos humanos han incorporado este derecho a sus textos y esto ha permeado los ordenamientos jurídicos y la jurisprudencia de los países[147].

Este ambiente global de información ha puesto en entredicho el concepto tradicional de *intimidad,* para dar paso a nuevos matices conceptuales, a nuevas perspectivas de comunicación entre las personas y los países, generando con ello nuevos retos para el derecho a la protección de datos, el cual se debate hoy día entre ligámenes a los viejos sistemas de control, y a la necesidad de utilizar nuevas

---

[146] SALDAÑA, M. N., "la protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de información personal en los Estados Unidos" en *Revista Aucaria,* vol. 9, No. 18, Sevilla, 2007, p. 87.

[147] El primer texto, de este tipo, que lo contempla es la Declaración Americana de Derechos y Deberes del Hombre de 2 de mayo de 1948, cuyo art. 5 establece que toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

herramientas tecnológicas para garantizar el derecho fundamental de los ciudadanos a decidir quién, cuándo y dónde, y bajo cuáles circunstancias, toma contacto con sus datos.[148]

Para Miguel Carbonel[149], podría hablase de violaciones a la intimidad en los siguientes casos: a) cuando se genere una intrusión en las esfera o en los asuntos privados ajenos, b) cuando se divulguen hechos embarazosos de carácter privado, c) cuando se divulguen hechos que suscitan una falsa imagen para el interesado, d) cuando se genere una apropiación indebida para provecho propio del nombre o de la imagen ajenos, e) cuando se revelen comunicaciones confidenciales.

El autor coincide con la mayoría de obras citados en que un aspecto esencial y peculiar de estos derechos es: la variabilidad de su ámbito de protección, lo cual está definido por el ámbito de acción de cada individuo, pero también puede depender de los diferentes regímenes sociales, políticos y económicos existentes, así como de los fenómenos y situaciones particulares de la vida privada de las personas.

En el caso de la información o la imagen de la persona, cada individuo tiene la facultad para disponer qué, cómo, cuándo y dónde se publica esta información. Esta facultad de disponibilidad puede ser aplicada también a la vida privada, sin embargo, pareciera no ser aplicable al derecho al honor. Debería entenderse que el

---

[148] CHIRINO SÁNCHEZ, A., *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica,* Comisión Nacional para el Mejoramiento de la Administración de Justicia, San José, 1997, p. 14.

[149] CARBONELL SÁNCHEZ, M., *Los derechos fundamentales en México,* UNAM-Porrúa-CNDH, 2005, pp. 450 y 455.

consentimiento es la clave, al menos para el derecho de información e imagen, para que se pueda disponer de estos derechos de forma legítima.

Del análisis histórico, relacionado con el desarrollo de este derecho, se puede apreciar que, el derecho de intimidad se definía como el derecho a ser dejado a solas o a la no intromisión en los asuntos personales o familiares de un individuo salvo que se autorice o se consienta la intromisión[150]; en la actualidad, se concibe como el derecho del individuo a decidir si desea compartir sus pensamientos, sentimientos y los hechos de su vida personal o familiar, por el acceso no autorizado a bases de datos que contengan información reservada. Pareciera que se trata de un derecho que en un principio tenía una condición prohibitiva a *no ser molestado* y luego se convierte en un derecho activo, en el cuál el individuo fija sus propios límites para consentir o autorizar el acceso a la información privada que desea hacer del conocimiento de las demás personas.

En la actualidad, varios ámbitos de protección integran el derecho de intimidad, lo que hizo crecer el contenido inicial de este derecho para proteger el conjunto de hechos y situaciones de la vida propia, que pertenecen a las personas como una reserva no divulgable, situándose cada uno de esos derechos como derechos autónomos, que para muchos juristas deriva del derecho de privacidad.

Estima Pérez Luño que este derecho rebasa los límites de las libertades individuales dado que presenta como condición la *existencia colectiva*, lo que no

---

[150] *Vid.* HERRERO-TEJEDOR quien sostiene que la *privacy* se configuró como un derecho de exclusión de los demás frente al ámbito privado, tratándose de una verdadera libertad negativa frente a la información abusiva, posteriormente, se concibe como una libertad positiva, al poder ejercer un control sobre los datos referidos a la persona, que han salido de la esfera de la intimidad para convertirse en elementos de un archivo electrónico privado o público. HERRERO-TEJEDOR, F., *Honor, intimidad y propia imagen*, Cólex, Madrid, 1990, p. 40.

debe ser ignorado en la reglamentación jurídica: *i.e.* que este derecho protege al individuo de la intervención de otras personas o de las instituciones.[151]

El desarrollo de la protección de ese derecho se refleja también en los instrumentos del derecho internacional, como producto quizá del avance tecnológico que se ha producido. El art. 1° del Convenio de Estrasburgo sobre la protección de las personas de 1981[152], en lo relativo al tratamiento automatizado de los datos de los datos de carácter personal, que uno sus fines es garantizar el derecho a la vida privada de las personas físicas en ese ámbito.

El reconocimiento a la vida privada y familiar, se introdujo también en la Declaración del Parlamento Europeo sobre Derechos y Libertades Fundamentales de 12 de abril de 1989[153], sin embargo, los intentos posteriores de conferir a esta declaración un estatuto jurídicamente vinculante resultaron infructuosos.

---

[151] *Vid.* PÉREZ LUÑO, A. E., *Derechos Humanos, Estado de Derecho… op. cit.,* pp. 324-325.

[152] *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.* Art. 1. Objeto y fin. El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»), [en línea], http://www.coe.int/t/dghl/standardsetting/dataprotection/Global_standard/Conv%20108_es.pdf. El Convenio 108 adoptado por la Comunidad Europea en 1981, es el primer instrumento internacional que procura reglar el fenómeno del tratamiento automatizado de datos correspondientes a personas naturales desde una perspectiva que trasciende a la legislación interna y cuyo contenido informaría a diversas legislaciones europeas originadas durante la década de los ochenta, con miras a disponer de una normativa comunitaria para hacer frente a una previsible proliferación de leyes nacionales que en su día hicieran difícil su armonización. Este Convenio fue ratificado por el Estado Español y, por tanto, válido y vigente en España, con rango ley desde el 1 de octubre de 1985.

[153] Sobre el papel de la Declaración de Derechos Fundamentales del Parlamento Europeo, se puede consultar en: http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_1.1.6.html

También se incluyó el reconocimiento en la Convención sobre los Derechos del Niño de 1989[154] y en la Convención de Derechos Humanos y Libertades Fundamentales de la Comunidad de Estados Independientes de 1995. En 1997, tras la aprobación del Tratado de Ámsterdam, el Parlamento volvió a solicitar la adopción de una Carta de los Derechos Fundamentales vinculante. Durante el proceso de elaboración que condujo a la adopción de la Carta, el Parlamento aprobó varias resoluciones en las que insistía en que este instrumento debía incorporarse a los Tratados para otorgarle un carácter jurídicamente vinculante[155].

Tras la proclamación solemne de la Carta, el Parlamento manifestó su decepción por su naturaleza no vinculante y pidió de nuevo que se incluyera en los Tratados de forma jurídicamente vinculante.

El 1 de diciembre de 2009[156], la Carta pasó a ser jurídicamente vinculante. Ahora, según el art. 6, apartado 1, del Tratado de la Unión Europea (TUE), "la Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea […], la cual tendrá el mismo valor jurídico que los Tratados". Por consiguiente, la Carta forma parte del Derecho primario de la Unión y, como tal, sirve de parámetro a la hora de examinar la validez del Derecho derivado y de las medidas nacionales.

---

[154] *Vid.* Art. 8 de la Convención sobre los Derechos del Niño de 1989, [en línea], http://www.unicef.org/argentina/spanish/7.-Convencionsobrelosderechos.pdf

[155] El Parlamento Europeo, el Consejo y la Comisión proclamaron solemnemente la Carta de los Derechos Fundamentales de la Unión Europea en Niza en el año 2000. Tras ser revisada, fue proclamada de nuevo en 2007.

[156] En el Título II, se confirman los derechos a la dignidad humana, la vida y la integridad de la persona, así como, la protección de los datos personales, ver arts. 7 y 8, [en línea], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:es:PDF

El concepto de dignidad aparece como parte de la condición humana y como fundamento de los derechos de la persona, independientemente, de su reconocimiento jurídico, situación que se entiende desarrollada al margen de los derechos admitidos a las personas. Dicho reconocimiento supone un gran avance en el desarrollo de los derechos fundamentales y libertades incluidos en las normas constitucionales, que además se deben interpretar en el marco de los derechos de los convenios y tratados de derechos humanos.

2.1.1.1. Control de convencionalidad americano.

El control de convencionalidad es un sistema diseñado por la Corte Interamericana de Derechos Humanos[157] y su acatamiento es de orden obligatorio para los Tribunales ordinarios y constitucionales, los que tienen el deber de constatar cualquier conducta (activa u omisiva) con el parámetro de convencionalidad o el *corpus iuris* interamericano, el cual se encuentra conformado por las convenciones y declaraciones regionales en materia de Derechos Humanos, la jurisprudencia de esa Corte y sus opiniones consultivas.

En la jurisprudencia de la Corte Interamericana de Derechos Humanos se ha conocido con el nombre de *control difuso de convencionalidad*, pare referirse a la labor de los jueces ordinarios con respecto a la "*misión de salvaguardar no sólo los derechos fundamentales previstos en el ámbito interno, sino también el conjunto de*

[157] Este control se encuentra dispuesto por la Corte Interamericana, principalmente, en las sentencias de los casos los casos Almonacid Arellano y otros c/. Chile de 26 de septiembre de 2006, Trabajadores Cesados del Congreso c/. Perú de 24 de noviembre de 2006, Cabrera García y Montiel Flores c/. México de 26 de noviembre de 2010 y Gelman c/. Uruguay de 24 de febrero de 2011. *Vid.* SSC No. 2013-10712 de las 11:31 hrs. del 8 de agosto de 2013.

valores, principios y derechos humanos que el Estado ha reconocido en los instrumentos internacionales y cuyo compromiso internacional asumió".[158]

El profesor Jinesta Lobo, Magistrado de la Sala Constitucional costarricense, comparte el criterio de la Corte Interamericana y hace la salvedad que los jueces y tribunales ordinarios están obligados a ejercer el control de convencionalidad en el marco de sus respectivas competencias y de las regulaciones procesales pertinentes, estimando que se otorga un margen de discrecionalidad judicial pero limitado por el ordenamiento jurídico interno o local[159]. Lo anterior también ha sido señalado en la sentencia de la Corte Interamericana de Derechos Humanos en el caso Almonacid y otros vs. Chile[160].

La teoría propuesta por la Corte Interamericana de Derecho Humanos, únicamente, podría resultar aplicable en los estados que permitan el control difuso de constitucionalidad, pues resulta evidente que en los casos en los cuales no se permita este control, los jueces no podrían dejar de aplicar el ordenamiento jurídico al caso concreto. Lo permitido para los jueces en esos casos sería realizar una interpretación conforme de la norma convencional según la Constitución nacional y la Convención Americana y de la jurisprudencia nacional. Al no poder desaplicar la norma al caso concreto, el juez tendría también la posibilidad de plantear un asunto o consulta de constitucionalidad ante el Tribunal Constitucional que posee el control

---

[158] FERRER MAC-GREGOR, E, voto razonado, caso Cabrera García y Montiel Flores vs. México, 2010, párrafo 24, p. 9, [en línea], http://www.corteidh.or.cr/docs/casos/articulos/seriec_220_esp.pdf

[159] JINESTA LOBO, Ernesto, "Control de convencionalidad ejercido por los Tribunales y Salas Constitucionales", en FERRER MAC-GREGOR, Eduardo (coord.), *El control difuso de constitucionalidad,* Fundap, México, 2012, pp. 7-8, [en línea], http://www.ernestojinesta.com/

[160] Corte Interamericana de Derechos Humanos, caso Almonacid y otros vs. Chile, 2006, [en línea], http://www.corteidh.or.cr/docs/casos/articulos/seriec_154_esp.pdf

concentrado de constitucionalidad para que emita el criterio solicitado, aspecto que si se encuentra autorizado en la experiencia costarricense[161].

En la resolución de cumplimiento sentencia del caso de Gelman vs. Uruguay de 2013[162], la Corte Interamericana de Derecho Humanos interpretó que la pretensión de oponer el deber de los tribunales internos de realizar el control de constitucionalidad al control de convencionalidad que ejerce la Corte, es en realidad un falso dilema, pues una vez que el Estado ha ratificado el tratado internacional y reconocido la competencia de sus órganos de control, precisamente a través de sus mecanismos constitucionales, aquéllos pasan a conformar su ordenamiento jurídico. De tal manera, el control de constitucionalidad implica necesariamente un control de convencionalidad, ejercidos de forma complementaria.

2.1.2. El Derecho de Intimidad en Costa Rica.

En Costa Rica, el derecho fundamental a la intimidad es tratado como un fuero de protección a la vida privada de los ciudadanos. La intimidad está formada por aquellos fenómenos, comportamientos, datos y situaciones de una persona que normalmente están sustraídos al conocimiento de terceros y cuyo conocimiento por éstos puede turbarla moralmente por afectar su pudor y su recato, a menos que esa misma persona consienta esa interferencia o acercamiento. De esta manera los derechos constitucionales de inviolabilidad del domicilio, de los documentos privados y de las comunicaciones existen para proteger dicha intimidad, que es un

---

[161] *Vid.* Art. 102 de la Ley No. 7135, Ley de la Jurisdicción Constitucional.

[162] Corte Interamericana de Derechos Humanos, sentencia de supervisión de cumplimiento de sentencia, caso Gelman vs. Uruguay, 2013, [en línea], http://www.corteidh.or.cr/docs/supervisiones/gelman_20_03_13.pdf

derecho esencial de todo individuo. Todos estos derechos solo ceden por causa justa.[163]

Sobre el **derecho a la intimidad**, el Tribunal Constitucional Costarricense, en SSC número 6776-94 de las 14:57 hrs. del 22 de noviembre de 1994, reconoció el derecho a la vida privada como la esfera en la cual nadie puede inmiscuirse. La libertad de la vida privada es el reconocimiento de una zona de actividad que es propia de cada uno y el derecho a la intimidad limita la intervención de otras personas o de los poderes públicos en la vida privada de la persona; esta limitación puede manifestarse tanto en la observación y captación de la imagen y documentos en general, como en las escuchas o grabaciones de las conversaciones privadas y en la difusión o divulgación posterior de lo captado u obtenido sin el consentimiento de la persona afectada.[164]

En lo que respecta a la **inviolabilidad de los documentos privados**, en SSC número 5685-95 de las 15:36 hrs. del 18 de octubre de 1995, relacionada con una Consulta Legislativa Preceptiva por la reforma del artículo 24 constitucional se dispuso:

"…los mismos pertenecen a la categoría de los llamados derechos "de libertad", que se refieren a las libertades formales que iniciaron su consagración como derechos en 1789 con la Declaración de los Derechos del Hombre y del Ciudadano. Comprenden todos aquellos derechos personales reconocidos por la tradición democrática liberal, como el derecho de participación en los asuntos públicos, la libertad de palabra, la libertad de imprenta, la libertad de conciencia, de

---

[163] SSC número 2012-3477 de las 14:30 hrs. del 31 de julio de 2012.

[164] SSC número 6776-94 de las 14:57 hrs. del 22 de noviembre de 1994. *"… el derecho a la vida privada se puede definir como la esfera en la cual nadie puede inmiscuirse. La libertad de la vida privada es el reconocimiento de una zona de actividad que es propia de cada uno y el derecho a la intimidad limita la intervención de otras personas o de los poderes públicos en la vida privada de la persona; esta limitación puede manifestarse tanto en la observación y captación de la imagen y documentos en general, como en las escuchas y grabaciones de las conversaciones privadas y en la difusión sin el consentimiento de la persona afectada*".

pensamiento, el derecho a la inmunidad personal, el secreto de la correspondencia, la inviolabilidad del domicilio, en fin, las condiciones establecidas en tutela del ciudadano contra el abuso del poder. Estos derechos, clasificados por algunos como los "derechos de la primera generación", son derechos que esencialmente implican una abstención por parte del Estado, cuya actuación es básicamente pasiva, pese a que supone no sólo un deber de garantizar el orden público dentro del cual esos derechos puedan aplicarse libremente y sin discriminaciones, sino además la necesidad de establecer y mantener las condiciones del orden dentro del cual se ejerzan esos derechos, para que existan efectiva y realmente. La obligación del Estado de Derecho con respecto a estos derechos, es esencialmente el no violarlos, si no intervenir en esa esfera íntima de los individuos, salvo las excepciones realmente calificadas en aras de tutelar el bien común, siempre en el entendido que los órganos contralores autorizados como excepción no contraríen otras garantías fundamentales. Estado de Derecho es entonces sinónimo de "galantismo", pues designa no simplemente un "Estado legal" o "regulado por la ley" sino que comprende un sentido sustancial que implica que todo poder debe estar limitado por la Constitución y la ley que condiciona no sólo su forma sino también su contenido, un modelo de Estado nacido con las modernas constituciones y caracterizado, en el plano formal, por el principio de legalidad, y en el plano sustancial, por la funcionalidad de todos los poderes del Estado en garantía de los derechos fundamentales de los ciudadanos, mediante la incorporación en su Constitución de los deberes públicos correspondientes. Por ello es necesario concebir la ley no como un producto del arbitrio, sino como el resultado de luna voluntad general encaminada directamente a garantizar los derechos de los individuos, sin que ello implique que la ley no pueda limitar o regular estos derechos de los individuos en protección de los derechos e intereses de cada uno de los miembros de una colectividad."

En lo que respecta al **derecho de imagen**, el artículo 47 del Código Civil Costarricense señala una excepción por la notoriedad de la persona. Esta excepción permite la divulgación de una imagen, sin el consentimiento de la persona, cuando *"dicha reproducción esté justificada por la notoriedad de aquella, por la función pública que desempeñe, por necesidades de justicia o de policía o cuando la*

reproducción se haga en relación con hechos, acontecimientos o ceremonias de interés público, o que tengan lugar en público" (artículo 47 del Código Civil)…"[165].

Varios principios pueden extraerse de la jurisprudencia de la Sala Constitucional Costarricense:

a) **Principio de limitación de objetivos, finalidad.** Los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse, únicamente, en cuanto ello no sea incompatible con el objetivo de la transferencia.
b) **Principio de proporcionalidad y de calidad.** Los datos deben ser exactos y estar actualizados, deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.
c) **Principio de transparencia.** Información en la recogida de los datos. Debe informarse a los interesados sobre el objetivo del tratamiento y de la identidad del responsable en el tercer país.
d) **Principio de seguridad.** El responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos.

2.1.3. El Derecho de Intimidad en España.

La intimidad personal y familiar puede considerarse como el reducto más privado de la vida del individuo, esto es, como aquéllos extremos más personales

[165] SSC número 2014-11715.

de su propia vida y de su entorno familiar, cuyo conocimiento está restringido a los integrantes de la unidad familiar.[166]

Sobre la naturaleza jurídica de los derechos fundamentales, el Tribunal Constitucional Español estima que cada derecho se configura estableciendo una relación entre el lenguaje de las disposiciones normativas y lo que algunos llaman el metalenguaje o las ideas generalizadas y convicciones admitidas, principalmente, entre los juristas, los jueces y, en general, los especialistas en Derecho, sobre lo que sea ese derecho[167]. De esta manera, constituyen el contenido esencial de un derecho subjetivo las facultades o posibilidades de actuación necesarias para que el derecho sea reconocible como pertinente al tipo descrito y sin las cuales deja de pertenecer a ese tipo y tiene que pasar a quedar comprendido en otro, con la consecuencia de la desnaturalización. Así la naturaleza jurídica o forma de concebir el derecho es uno de los caminos que permite la aproximación a su contenido esencial.

La titularidad de los derechos relacionados con la intimidad, al igual que todos los derechos de la personalidad, la ostentan todas las personas y se trasladan al ámbito familiar, entendida la familia en sentido amplio. Los derechos de intimidad y honor se pueden trasladar a personas jurídicas.

En cuanto a la intimidad, el Tribunal Constitucional Español, señaló que se trata de un derecho que afecta sólo a las personas físicas, lo que parece acorde con el propio sentido de los términos empleados por la Constitución Española (STC

---

[166] LÓPEZ GUERRA, L., ESPÍN TEMPLADO, E., GARCÍA MORRILLO, J., PÉREZ TREMPS, P., y SATRÚSTEGUI, M., *Derecho Constitucional,* Tirant lo Blanch, vol. I, 9ª ed., Valencia, 2013, [versión para lector digital Kindle].

[167] FERNÁNDEZ ACEBO, M. D., "La tutela de los derechos fundamentales a la intimidad e integridad física frente a la actuación de los poderes públicos sobre el cuerpo humano. Una perspectiva constitucional sobre las intervenciones corporales y otras diligencias de investigación", *Tesis Doctoral,* Universidad de A Coruña, 2013, p. 59.

137/85, caso Derivados de Hojalata, S.A.). Respecto al **derecho al honor**, el Tribunal Constitucional Español, subrayó su contenido, primariamente, personalista (STC 107/88, caso Objetor de conciencia), no se ven obstáculos de importancia a que las personas jurídicas o al menos algunas de ellas, para las que la reputación pueda ser decisiva, vean constitucionalmente garantizados su buen nombre y reputación, quedando así protegidas de la difamación o de expresiones ofensivas e injuriosas. Y, efectivamente, el Tribunal Constitucional, en una importante sentencia (STC 139/95, caso Honor de personas jurídicas), atribuyó la **titularidad del derecho a las personas colectivas**. En todo caso, el rigor de protección siempre será menos intenso y riguroso que en el caso de las personas físicas.[168]

En cuanto a la intimidad personal, el ATC 257/1985 de 17 de abril[169], señala en su fundamento jurídico 2º que el derecho a la intimidad que reconoce el art. 18.1 de la Constitución, por su propio contenido y naturaleza, se refiere a la vida privada de las personas individuales, en la que nadie puede inmiscuirse sin estar debidamente autorizado, y sin que en principio las **personas jurídicas puedan ser titulares del mismo**.

Las primeras referencias importantes sobre el derecho a la protección de datos personales en la península ibérica se encuentran reconocidos, en un inicio, en los trabajos preparatorios del artículo 18.4 de la Constitución Española de 1978 y, en la actual Ley Orgánica de Protección de Datos Personales de 13 de diciembre de 1999.[170]

---

[168] LÓPEZ GUERRA, L., *et. ál.*, *op. cit.,* [versión para lector digital Kindle].

[169] *Vid.* STC, Sección Segunda. Auto 257/1985, de 17 de abril de 1985.

[170] Uno de los antecedentes que posiblemente influyó sobre el Constituyente Español en la composición de este artículo relativo a la regulación de los datos personales y la informática fue el

Se podría estimar que la protección de tal derecho fue garantizado, desarrollado y protegido, en un primer momento, en el marco de Convenios Internacionales suscritos por España. Siguiendo esos avances muy de cerca, el propio Tribunal Constitucional lo hacía con ocasión de tramitar y fallar en un proceso de amparo constitucional, esto ante la ausencia de una ley interna que desarrollara tal mandato. Posteriormente este derecho es garantizado por la Ley Orgánica de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen de 1982; diez años más tarde, por una Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) para, finalmente, en 1999, perfeccionarse la protección en una Ley de Protección de Datos de Carácter Personal que permanece vigente a la fecha, cuya ejecución se regula por el Real Decreto 1720/2007, de 21 de diciembre, en el cual se abordan aspectos procesales con más y mayor especificidad que lo dispuesto en la ley que desarrolla.

Mediante la Ley Autonómica 13/1995, de 21 de abril, dictada por la Comunidad de Madrid, se creó y puso en funcionamiento la Agencia de Protección de Datos de Madrid[171]. Posteriormente, se creó la Agencia Catalana de Protección de Datos (APDCAT)[172], mediante Ley 5/2002, de 19 de abril, iniciando sus

---

artículo 35 de la Constitución de Portugal de 1976, el cual establecía: 1. Todos los ciudadanos tendrán derecho a tener conocimiento de lo que conste en forma de registros automatizados acerca de ellos y de la finalidad a que se destinan las informaciones, y podrán exigir la rectificación de los datos, así como su actualización. 2. No se podrá usar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos. 3. Se prohíbe atribuir un número nacional único a los ciudadanos.

[171] *Vid.* Agencia Española de Protección de Datos (AEPD), consultable en: http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

[172] *Vid.* Agencia Catalana de Protección de Datos (APDCAT), consultable en: http://www.apd.cat/es

actuaciones en octubre 2003. El País Vasco por medio de la Ley 2/2004, de 25 de febrero, Ley de Ficheros de Datos de Carácter Personal de Titularidad Pública, creó la Agencia Vasca de Protección de Datos (AVPD).[173]

Podría afirmarse que fue hasta la entrada en vigor de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, conocida como LORTAD que, finalmente, da cumplimiento al mandato constitucional del artículo 18.4 de la Constitución y a las obligaciones internacionales contraídas por España tras la ratificación del Convenio 108 del Consejo de Europa.

La incorporación de la Directiva 95/46/CE[174] al ordenamiento jurídico español comporta un cambio radical en la regulación de los supuestos internacionales de tratamiento automatizado de datos de carácter personal, al grado de que la adecuación de la normativa interna se vería comprometida sustancialmente y se dictaría a la postre una legislación totalmente nueva acorde con los principios informadores de esta Directiva; la LOPD.

---

[173] *Vid.* Agencia Vasca de Protección de Datos (AVPD), consultable en: http://www.avpd.euskadi.eus/s04-5213/es/

[174] La Directiva parte de considerar que *"los sistemas de tratamiento de datos están al servicio del hombre"* y que deben *"respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad"*. Busca una libre circulación de los datos garantizando los derechos fundamentales. Así lo establece el considerando 8, cuando dice que *"para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros"*. En el art. 1 se obliga a los Estados miembros a garantizar la intimidad frente al tratamiento de datos personales y el art. 2 se dedica a las definiciones, que luego se incorporarán a la normativa nacional. Se consagran los principios relativos a la calidad de los datos, como el principio de lealtad, de fin legítimo, de adecuación, de exactitud y de conservación (art. 6); y los principios relativos a la legitimación del tratamiento de datos (art. 7), como el de consentimiento.

2.1.4. El Derecho de privacidad en EE.UU.

En el apartado 3.2 del capítulo II *supra*, se señalaron partes importantes sobre el origen de la protección de la privacidad en el derecho de los EE.UU. Dadas la características propias del derecho común (*Common law*), la protección principal del derecho de privacidad, está contenida, fundamentalmente, en los precedentes jurisprudenciales.

El derecho a la *privacy* no está reconocido de manera expresa en la constitución, sin embargo, su protección es inferida de ese texto, pero si está reconocida en leyes de agravios civiles, por la cual se entiende que cualquiera que invada intencionadamente, física u otra forma la privacidad de otra persona, en lo que se refiere a sus asuntos privados, queda sujeto a la responsabilidad por invasión de la intimidad (*torts law*).

Esta protección se ha extendido y se aplica a todo lugar privado, se puede aplicar también a los archivos informáticos guardados en un lugares privados, así como, a las escuchas telefónicas y a la intercepción del correo personal[175].

La forma de protección en EE.UU., al igual que en la mayoría de países que emplean el sistema de derecho continental, se ha extendido para dar protección a "nuevas" formas en las cuales se podría vulnerar este derecho. Si bien en los orígenes de la *privacy* se considera que la protección parte del planteamiento de Warren y Brandeis, hoy día se ha ampliado considerando otras formas de protección, entre las cuales se protegen los archivos y ficheros informáticos y las comunicaciones, aparte de las formas tradicionales de protección ya utilizadas desde hace muchos años.

---

[175] CASTILLO JIMENES, C., "Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información", *En Derecho y Conocimiento*, vol. 1, Facultad de Derecho de la Universidad de Huelva, [en línea], http://www.uhu.es/derechoyconocimiento/DyC01/A02.pdf

Si bien en los EE.UU. la protección del derecho de privacidad, no está contenido de forma expresa, se infiere del texto de las Constitución y se encuentran protegido por la Ley de Agravios (torts law) de forma inicial, sin embargo, se ha desarrollado la protección de este derecho en una serie de normas relacionadas, a través de las cuales se protegen los archivos y ficheros informáticos y las comunicaciones, aparte de las formas tradicionales de protección ya utilizadas desde hace muchos años.

Las leyes de agravios a la privacidad en los EE.UU. protegen únicamente en cuatro situaciones:

1. La intrusión en asuntos de la vida privada de otro;

2. La apropiación del nombre o imagen del otro;

3. La divulgación de la vida privada de los demás;

4. La publicidad que coloca injustificadamente a otro en una falsa luz ante el público.

2.1.4.1. Ley de responsabilidad civil por agravios a la privacidad *(the privacy torts*).[176]

En EE.UU., la ley civil ha sido la primera línea de defensa de la privacidad a nivel estatal. Por su naturaleza, los límites particulares de esta área de la ley, varían de un estado a otro, a veces de forma dramática. Algunos estados reconocen los cuatro intereses de la privacidad, otros, por el contrario, solo aceptan algunos de

[176] *Vid.* Ley de acciones o agravios civiles a la privacidad, *Restatement (Second) of Torts*, §§ 652A-E, [en línea], http://www.tomwbell.com/NetLaw/Ch05/R2ndTorts.html

estos, por ejemplo, Minnesota y Texas aceptan sólo tres de estos intereses[177], desconociendo el agravio de publicaciones falsas frente a terceros (*false light*)[178].

En general, las leyes de responsabilidad por agravios (*torts law*), reconocen cuatro tipos diferentes de protección de la privacidad (*privacy torts*)[179]:

1. La **intrusión** en asuntos de la vida privada de otro;
2. La **apropiación** del nombre o imagen del otro;
3. La **divulgación** de la vida privada de los demás;
4. La publicidad que coloca injustificadamente a otro en una **falsa luz** ante el público.[180]

a) **La intrusión.**

A diferencia de los otros tres agravios o acciones, esta no requiere la divulgación, se trata de la recopilación no autorizada de la información de la vida privada de otra persona. Es el acto de invasión de la privacidad de un individuo en

---

[177] SOLOVE, D. J. y SCHWARTZ P. M., *Privacy Law Fundamentals*, IAPP Publications, 3era edición, New Haven, 2015, p. 26.

[178] El Estado de Minnesota, no acepta los cuatro intereses de la *privacy*, según se expresó en el caso Lake v. Wal-Mart, 582 N.W.2d 231 (Minn. 1998), en el cual el Tribunal Supremo de Minnesota señaló no amparar los casos de privacidad por el delito de publicaciones falsas (false light), aunque si reconocía el derecho fundamental a la privacidad, lo anterior por cuanto se contrapone a la libertad de expresión, tutelada constitucionalmente.

[179] SOLOVE, D. J., *The digital person. Technology and privacy in the information age,* New York University Press, New York and London, 2004, [versión para lector digital Kindle]; HANKIN, R., *Invasion of privacy & the law*, Looseleaf Law Publications, New York, 2013, [versión para lector digital Kindle]; SOMA, J. T., RYNERSON, S. D. y KITAEV, E., *Privacy Law*, Editorial West, Minnesota, 2014, [versión para lector digital Kindle].

[180] Este agravio es el más criticado de los cuatro. La Corte Suprema de Texas también ha negado la tutela de este agravio, al efecto se pueden consultar los casos Sullivan v. Pulitzer Broadcasting Co., 709 S.W.2d 475 (Mo. 1986); Renwick v. News and Observer Pub. Co., 312 S.E.2d 405 (N.C. 1984); Cain v. Hearst Corp., 878 S.W.2d 577 (Tex. 1994).

sus asuntos privado o su soledad. Esta invasión podría ser visual y auditiva y puede ser de forma física o electrónica.[181]

La responsabilidad civil por intromisión en la reclusión recoge las prácticas invasivas de recolección de información. Esta requiere que el demandante demuestre que el demandado (a) intencionalmente se inmiscuyó, físicamente o de otra manera, (b) en la reclusión o soledad de otro o en sus asuntos o problemas privados, (c) en una manera altamente ofensiva a una persona. Esta acción civil se aplica a situaciones donde la información es descubierta de una manera furtiva en un lugar privado y permite al perjudicado el resarcimiento daños y perjuicios ocasionados por la invasión en su reclusión o soledad. La acción, claramente, comprende invasiones no-físicas como aquellas que son "intrusiones sensoriales injustificadas como la interceptación telefónica, electrónica, y el espiar visual o fotográficamente".[182]

b) **La apropiación del nombre o la figura.**

Este agravio se refiere al acto de apropiación del nombre o imagen de una persona cuando representa una ventaja para la otra. Protege contra la apropiación de la identidad de una persona, sin su consentimiento, para hacer publicidad.[183]

La acción por apropiación es entendida, únicamente, como una violación a la propiedad. La acción no se dirige frente a medios intrusivos de colección de

[181] SOMA J. T., RYNERSON S. D. y KITAEV E., *op. cit.*, [versión para lector digital Kindle].

[182] ABRIL, P. S., y PIZARRO MORENO, E., "La intimidad europea frente a la privacidad americana. Una visión comparativa del derecho al olvido" en *InDret Revista para el análisis del derecho*, Barcelona, enero 2014, p.18, [en línea], http://derechoaleer.org/media/files/olvido/1031.pdf

[183] SOMA J. T., RYNERSON S. D. y KITAEV E., *op. cit.*, [versión para lector digital Kindle].

información o de difusiones vergonzosas. Por el contrario, se enfoca en el uso comercial no autorizado de la identidad de una persona y sus consecuentes daños a la dignidad. La pretensión contenida en una demanda civil amparada en esta acción está basada en reconocer que un individuo tiene un interés o derecho de propiedad sobre su nombre o figura. La acción se aplica cuando la información de la persona o su imagen es usada sin su consentimiento para los propósitos comerciales del demandado.[184]

c) **La falsa luz o distorsión de la imagen.**

Este agravio, se refiere al acto de colocar a un individuo ante una falsa luz ante los ojos del público. Por lo general se trata de tergiversar declaraciones de una persona, en especial cuando ello afecta a la persona. Este agravio parece similar a la difamación. En el caso de la difamación se requiere que la información publicada sea falsa, en el caso de la luz falsa, la información es precisa pero crea una impresión errónea acerca de la persona.[185]

Es decir, si las leyes sobre difamación protegen la reputación del individuo, la acción por distorsión de la imagen se enfoca en reparar el daño causado a la paz mental del individuo. Esta acción se concentra en determinar si la información publicada, sobre un individuo, es falsa o engañosa, de manera que haya sido diseminada con conocimiento de su falsedad y tiene que ser considerada altamente ofensiva. Al igual que las otras acciones debe involucrar información privada. Además, protege también en los casos en que la información fue colocada en un

---

[184] ABRIL, P. S., y PIZARRO MORENO, E., *op. cit.,* p. 18.

[185] SOMA J. T., RYNERSON S. D. y KITAEV E., *op. cit.,* [versión para lector digital Kindle].

lugar público, es decir, los casos en los cuales la información no fue publicada pero fue colocada a la vista de otras personas.[186]

d) **La divulgación o difusión pública de hechos privados.**

Este agravio también es conocido como la *publicación indebida de hechos privados*. Consiste en el acto de dar a conocer hechos privados o embarazosos de una persona. Por ejemplo, las relaciones sexuales, el contenido de personal de cartas, peleas familiares, tratamientos médicos y fotografías de una persona en su casa, lo cual ha sido clasificado por parte de los tribunales como *hechos privados.* Este derecho exige cuatro elementos: a) que la difusión de la información sea verdadera; b) que resulte ofensiva para una persona razonable; c) que no sea de interés público; y, d) que la publicación sea tan íntima que afecte el sentido de la decencia[187].

La acción de difusión pública de hechos privados da lugar a una compensación por la publicación injustificada de hechos verdaderos, pero sin valor informativo, privados, y ofensivos. Evidentemente, cuando la información ha sido difundida o expuesta públicamente no puede existir una expectativa de privacidad. Además, debe entenderse que la libertad de expresión no se ve limitada cuando las publicaciones o difusiones de información se sustentan en asuntos con interés público o de valor informativo a pesar de que sean privados por naturaleza. Estos

---

[186] ABRIL, P. S., y PIZARRO MORENO, E., *op. cit.,* p. 19.

[187] SOMA J. T., RYNERSON S. D. y KITAEV E., *op. cit.,* [versión para lector digital Kindle].

requisitos suponen una barrera significativa para los demandantes y la obtención de daños en demandas por acciones derivadas de la violación a la privacidad[188].

2.1.4.2. La Constitución de EE.UU.

La Constitución de los EE.UU. protege la privacidad de varias formas distintas pese a no utilizar la palabra privacidad en el documento[189]. De esta manera, aunque la protección del derecho no se da de forma expresa en el texto de la constitución, se protegen varias dimensiones de la vida privada, las que han sido modeladas por la Corte Suprema de los EE.UU.

Las constituciones de algunos de los Estados de EE.UU. señalan de forma explícita la protección del derecho de privacidad. Este derecho se puede observar

[188] ABRIL, P. S., y PIZARRO MORENO, E., op. cit., p. 19.

[189] SOLOVE, D. J., *The digital person. Technology and privacy …, op. cit.,* [versión para lector digital Kindle].

en las constituciones de Alaska[190], California[191], Florida[192], Arizona[193], Montana[194], Hawái[195], Illinois[196], Carolina del Sur[197], Luisiana[198] y Washington[199].

---

[190] *Constitution of the State of Alaska*, art. I sec. 22. *Right of Privacy. The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.* [Amended 1972]. La Constitución del Estado de Alaska, art. I párrafo 22. Derecho a la Privacidad. El derecho de las personas a la privacidad es reconocido y no debe ser infringido. Se implementará esta sección mediante la ley [traducción libre del autor].

[191] *Constitution of the State of California,* art. I, sec. 1, 3. 3, 24, 28.8.1. *All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.* Todas las personas son por naturaleza libres e independientes y tienen derechos inalienables. Entre estos están el disfrute y defensa de la vida y libertad, adquirir, poseer y protección de la propiedad y la búsqueda y obtención de la seguridad, la felicidad y la privacidad [traducción libre del autor].

[192] *Constitution of the State of Florida*, art. I, sec. 23. *Right of privacy. Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.* Todas las personas físicas tienen el derecho a ser dejados a solas y tienen la libertad de intrusiones gubernamentales en la vida privada, salvo las disposiciones en contrario de este documento. Esta sección no se interpretará como una limitación del derecho público de acceso a los registros públicos y reuniones previstas por la ley [traducción libre del autor].

[193] *Constitution of the State of Arizona*, art. II sec. 8. *Right to privacy. No person shall be disturbed in his private affairs, or his home invaded, without authority of law.* Derecho de Privacidad. Nadie podrá ser molestado en sus asuntos privados, o la invasión de si hogar, sin autoridad de la ley [traducción libre del autor].

[194] *Constitution of the State of Montana*, art. II sec. 10. *Right of privacy. The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.* Derecho de Privacidad. El derecho de la privacidad individual es esencial para el bienestar de una sociedad libre y no será infringido sin la demostración de un interés apremiante del Estado [traducción libre del autor].

[195] *Constitution of the State of Hawaii*, art. I, sec. 6. *The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right.* El derecho del pueblo a la vida privada es reconocido y no podrá se violado sin la demostración de un interés apremiante del Estado. La legislación deberá adoptar medidas para implementar este derecho [traducción libre del autor].

[196] *Constitution of the State of Illinois,* art. I, sec. 6, 12. SEARCHES, SEIZURES, PRIVACY AND INTERCEPTIONS. The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of

communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly describing the place to be searched and the persons or things to be seized. BUSQUEDAS, ATAQUES, PRIVACIDAD E INTERCEPTACIÓN. Los ciudadanos tienen el derecho a que se les asegure, sus domicilios, documentos y otras posesiones contra registros irrazonables, ataques, invasiones a la privacidad o interceptación de dispositivos de comunicaciones y otros medios. No se expedirá una orden judicial sin una causa probable, apoyada por la declaración jurada particular describiendo el lugar a ser registrado y las personas o cosas contra las cuales se investigará [traducción libre del autor].

[197] *Constitution of the State of South Carolina,* art. I, sec. 10. *Searches and seizures; invasions of privacy. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, the person or thing to be seized, and the information to be obtained.* Allanamientos y decomisos; invasión de la privacidad. El derecho de las personas a la seguridad para no permitir la violación de sus, domicilios, documentos y otros efectos contra registros e incautaciones irrazonables e invasiones injustificadas de privacidad, y no se expedirá una orden judicial sin una causa probable, apoyada por la declaración jurada o afirmación describiendo el lugar a ser registrado y las personas o cosas contra las cuales se investigará, y la información que se obtenga [traducción libre del autor].

[198] *Constitution of the State of Louisiana,* art. I sec. 5. Right to Privacy. Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy. No warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful purpose or reason for the search. Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court. Derecho de privacidad. Debe asegurarse a todas las personas su propiedad, comunicaciones, casas, documentos y efectos contra registros irrazonables, ataques o invasión de la privacidad. No se emitirá orden judicial sin causa probable apoyada en juramento o protesta y describan particularmente el lugar que deba ser registrado, las personas o cosas que hay que investigar, y el propósito legal o el motivo de la búsqueda. Cualquier persona adversamente afectada por un registro o incautación realizada en violación de lo señalado en esta sección podrá amparar la ilegalidad en el tribunal correspondiente [traducción libre del autor].

[199] *Constitution of the State of Washington,* art. I sec. 7. *INVASION OF PRIVATE AFFAIRS OR HOME PROHIBITED. No person shall be disturbed in his private affairs, or his home invaded, without authority of law.* PROHIBÍDA LA INVASIÓN DEL HOGAR O ASUNTOS PRIVADOS. Nadie podrá ser molestado en sus asuntos privados, o la invasión de su domicilio, sin autoridad de la ley [traducción libre del autor].

a) **La Primera Enmienda de la Constitución de los EE.UU.**

En esta se protegen los derechos a la libertad de religión y la libertad de expresión, a partir de la interferencia del gobierno.

Con respecto al derecho de privacidad, esta Enmienda también, protege la libertad de asociación de las personas. Este derecho protege a las organizaciones restringiendo el derecho del gobierno para revelar los nombres y direcciones de sus miembros y para obligar a las personas a señalar las organizaciones a las cuales pertenecen[200].

La Corte Suprema de los EE.UU.[201] ha señalado que el derecho a la privacidad es esencial para el derecho de asociación, puesto que permite a las personas unirse sin tener que temer por la pérdida del empleo, huir de su comunidad u otros reproches sociales[202].

Difícilmente, pueda ser protegido el derecho de anonimato con respecto a la pertenencia a organizaciones, pues cada vez es más fácil acceder a los registros telefónicos, correos electrónicos o registros digitales de las personas.

La Primera Enmienda también se puede oponer en dos sentidos ante los requerimientos por parte del gobierno frente a información de las personas; el

---

[200] SOLOVE, D. J., *The digital person. Technology and privacy* …, op. cit., [versión para lector digital Kindle].

[201] *Vid.* Corte Suprema de los EE.UU. NAACP v. Alabama, 357 U.S. 449 (1958); Shelton v. Tucker, 364 U.S. 479 (1960).

[202] *SOLOVE, D. J., The digital person. Technology and privacy …, op. cit.,* [versión para lector digital Kindle].

primero, sobre la identidad de personas que se expresan de forma anónima y; el segundo, ante la coacción gubernamental para obtener información[203].

b) **La Cuarta Enmienda de la Constitución de los EE.UU.**

La Cuarta Enmienda[204] restringe a las agencias gubernamentales frente a los registros e incautaciones irrazonables, salvo los casos de excepción. Aplica inicialmente a la idea *each man's home is his castle* (la casa de cada hombre es su castillo), para protegerse frente a las pesquisas y aprehensiones arbitrarias de la propiedad por parte de las autoridades del gobierno. Esta enmienda, se constituye como la base para la órdenes de registro y detención, inspecciones de seguridad, escuchas telefónicas y otras formas de vigilancia[205], siendo la base fundamental de muchos otros temas de la ley penal y las leyes de privacidad.

El reclamo ante las requisas o incautaciones por parte de agentes federales es llamado "bivens actions"[206], término generado por la Corte Suprema de los

---

[203] *Ibíd.*

[204] *Constitution of the United States, Amendment IV*, *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*. El derecho de los habitantes de que sus domicilios, documentos y efectos contra registros e incautaciones irrazonables, no sean violados, y no se podrá emitir una orden judicial de allanamiento si no existe causa probable, apoyada por juramento o protesta y particularmente describiendo el lugar para ser registrado y las personas o cosas que hay que investigar [traducción libre del autor].

[205] Si bien la Cuarta Enmienda protege de otros tipos de vigilancia, como la electrónica, existen Leyes que hacen casi nugatorio este derecho al permitir una disminución de garantías como la Ley de Vigilancia de Inteligencia Extranjera por sus siglas en inglés (FISA) de 1978 y la Ley Patriota de 2001. Estas leyes serán analizadas a profundidad en el capítulo VI.

[206] *Corte Suprema de los EE.UU.,* caso Bivens v. Six Unknown Named Agents 403 U.S. 388 (1971), en el cual se demostró la violación de los derechos de la Cuarta Enmienda causados por un allanamiento. *Cfr.* PFANDER, J.E., *The Story of Bivens v. Six Unknown-Named Agents of the Federal Bureau of Narcotics*, Northwestern University School of Law, 2009, [en línea],

EE.UU. en la jurisprudencia. Hoy días las acciones *Bivens* se refieren a todas las acciones por daños y perjuicios cuando se ha producido una violación de la Constitución de los EE.UU. por parte de agentes federales. De todas maneras, aunque existe la protección, el Presidente de los EE.UU.[207] tiene el derecho de absoluta inmunidad frente a las acciones *Bivens*.

El derecho de la Cuarta Enmienda, no aplica a la información colectada por el gobierno o sus agencias en campos abiertos[208] de propiedad privada, puesto que no existe una expectativa de privacidad en estos lugares, salvo algunas excepciones, como por ejemplo, el caso del Estado de Oregon, en el cual se estimó que los lugares circundantes de una propiedad privada necesitan de una orden para el registro e incautaciones.

Evidentemente, se puede renunciar a los derechos tutelados en la Cuarta Enmienda. El consentimiento, o la falta de oposición, ante una búsqueda o incautación podrían excluir la tutelad de este derecho.

Louis Brandeis se basó en la Cuarta y Quinta Enmiendas a la Constitución de los EE.UU. para delimitar el derecho a la privacidad como un instituto jurídico.

---

http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1188&context=facultyworkingpapers

[207] *Corte Suprema de los EE.UU.,* caso Nixon v. Fitzgerald 457 U.S. 731 (1982).

[208] La excepción de la aplicación de la Cuarta Enmienda en campos abiertos fue desarrollada en el caso de la *Corte Suprema de los EE.UU.* Hester v. United States 265 U.S. 57 (1924).

c) **La Quinta Enmienda de la Constitución de los EE.UU.**

Esta Enmienda se refiere a la limitación del gobierno para obligar a las personas a revelar información incriminatoria en su contra. La Quinta Enmienda, protege de alguna manera el derecho a la privacidad.

Más allá de una disposición expresa por parte de la Constitución para la protección de la privacidad, la Corte Suprema ha señalado que esta se protege de forma explícita[209]. En el caso Griswold[210] se sientan las bases para una serie de casos relacionados con libertades individuales, referidos al sexo, al matrimonio y a la familia, y que dejarían un impacto en decisiones históricas como Roe v. Wade[211] y Lawrence v. Texas.[212]

La Cuarta y Quinta Enmienda protegen contra las infracciones del Gobierno, y no hacen nada para el control de la recolección y uso de información por parte de las burocracias privadas. A pesar de lo anterior no se aplica al sector privado, la Cuarta Enmienda tiene el potencial de proteger contra el uso de los ficheros digitales[213].

---

[209] *Vid.* Corte Suprema de los EE.UU. caso Griswold v. Connecticut 381 EE.UU. 479 (1965).

[210] *Ibíd.*

[211] *Corte Suprema de los EE.UU.* caso Roe v. Wade 410 U.S. 113 (1973), en el cual Tribunal sostuvo una posición de protección para las mujeres embarazadas que desean practicar un aborto y su derecho a la privacidad en los casos en los cuales esta posibilidad es permitida en relación con el avance del embarazo.

[212] *Corte Suprema de los EE.UU.* caso Lawrence v. Texas 539 U.S. 558 (2003), en el Tribunal mantiene una posición de mayoría para la protección de las relaciones íntimas entre personas dentro de su hogar.

[213] SOLOVE, D. J., *The digital person. Technology and privacy* …, *op. cit.,* [versión para lector digital Kindle].

En el caso Whalen v. Roe[214] en 1977, la Corte Suprema extendió el debido proceso a la protección de la privacidad de la información. En este caso, el Estado de Nueva York, aprobó una ley que requiere el registro de las personas que hayan obtenido medicamentos adictivos. La decisión del Tribunal se basó en la existencia de un riesgo ante la posibilidad de divulgación accidental lo cual sería una invasión a la privacidad.

Se estima que este caso renueva el derecho a la privacidad en el derecho constitucional conocido como privacidad de la información[215].

Otras formas de protección de la vida privada de las personas han sido protegidas a través de la jurisprudencia de la Corte Suprema de los EE.UU. extendiendo la protección a varias de las dimensiones.

Se han aprobado más de 20 leyes relacionadas con la privacidad en los EE.UU., protegiendo algunas situaciones particulares de algunos ámbitos de la privacidad. Sin embargo, las normas también señalan excepciones o limitaciones de este derecho, que a efectos de esta investigación tiene mucho interés dado que algunas de estas sirven de base para que las agencias de inteligencia hayan desarrollado programa de vigilancia masiva electrónica.

Entre las normas que han permitido la recogida de datos a granel, se encuentran: La ley de vigilancia extranjera (Foreign Surveillance Act) de 1978, que fue reformada por Ley Patriota (USA-Patriot Act) de 2001, luego de los ataques terroristas que sufrió los EE.UU. el 11 de setiembre y la Ley de Libertad de los

---

[214] *Corte Suprema de los EE.UU.* caso Whalen v. Roe 429 U.S. 589 (1977).

[215] SOLOVE, D. J. y SCHWARTZ P. M., *Privacy, information and technology*, Wolters Kluwer Law, 3era edición, Maryland, 2011, p. 35.

EE.UU. (Freedom Act) de 2015, que termina reformando ambas leyes luego del escándalo tras las revelaciones de Edward Snowden.

2.1.4.3. Leyes de protección de la privacidad.

En el presente apartado se plantea una sistematización de las leyes de los EE.UU. relacionadas con la privacidad de las personas. Este planteamiento tiene dos propósitos principales, el primero es mostrar la cantidad y la especialidad de la normativa aprobada y, en segundo lugar, permite ubicar la normativa sobre la cual se harán un análisis en los siguientes capítulos.

Según Solove desde 1970 el Congreso de los EE.UU. ha aprobado más de 20 leyes relacionadas con la privacidad[216]. A diferencia de la Unión Europea, que ha adoptado una directiva general para la protección de la privacidad[217], en los EE.UU. no se han promulgado normas de alcance similar. En su lugar, el Congreso ha aprobado una serie de estatutos adaptados a la medida de algunos problemas específicos de la privacidad, pero con algunas dificultades para cubrir todos los supuestos en los cuales se puede vulnerar la privacidad y de poca aplicación práctica.

Tal y como se indicó, se propone una sistematización basada en la aportada por Daniel Solove[218], en la cual se exponen las normas federales relacionadas con la privacidad:

---

[216] SOLOVE, D. J., *The digital person. Technology and privacy* …, *op. cit.,* [versión para lector digital Kindle].

[217] *Vid.* Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre del 1995.

[218] SOLOVE, D. J., *The digital person. Technology and privacy* …, *op. cit.,* [versión para lector digital Kindle]. También se pueden consultar: ALLEN, A. L., *Unpopular Privacy: What must we hide?,* Oxfort University Press, New York, 2011, [versión para lector digital Kindle]; HANKIN, R., *Invasion of privacy*

a) **Fair Credit Reporting Act (FCRA) of 1970[219].**

Regula la información de las agencias protectoras de datos de crédito, sin embargo, no restringe los usos secundarios y revelaciones de información. Esta normativa permite la venta de historiales crediticios que contiene información personal como nombres, direcciones actuales y anteriores, teléfono, números de seguridad social, empleo y fecha de nacimiento. No protege para igualar la desequilibrada relación de poder entre las compañías protectoras de crédito y las personas.

Entre los supuestos en los que pueden realizarse informes personales sobre créditos, destacan el consentimiento del consumidor para fines concretos, la concesión de créditos, la obtención de empleo, la contratación de seguros, los procedimientos administrativos en el ámbito de la tutela de menores y, por supuesto, la existencia de un mandato judicial. La ley permite a los consumidores inspeccionar sus datos bancarios, teniendo derecho a saber lo que hay en su expediente (divulgación del expediente) y conocer si la información registrada en su expediente ha sido utilizada en su contra. Asimismo, la ley permite inspeccionar y corregir información incompleta o imprecisa, debiéndose eliminar o corregir la información imprecisa, incompleta o que no se pueda verificar en el plazo de 30 días. Fue modificada en el año 2005, los derechos garantizados se protegen a través de los daños y perjuicios. Las excepciones planteadas en esta normativa han hecho

---

& the law, Looseleaf Law Publications, New York, 2013 [versión para lector digital Kindle]; RUSTAD, M. L., *Global Internet law*, editorial West, segunda edición, Minnesota, 2013, [versión para lector digital Kindle]; SOMA, J. T., RYNERSON, S. D. y KITAEV, E., *Privacy Law*, Editorial West, Minnesota, 2014, [versión para lector digital Kindle]; SOLOVE, D. J. y SCHWARTZ, P. M., *Privacy Law Fundamentals,* IAPP Publications, 3era edición, New Haven, 2015.

[219] Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. § 1681, [en línea], http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf

ineficaz la protección de la información de las personas, razón por la cual los Estados han regulado el tema a nivel local.

b) **Privacy Act of 1974[220].**

Esta normativa es considerada como una de las más importantes de los años setentas y regula la recopilación y uso de la información por parte de las agencias federales, permitiendo a los individuos acceder y corregir la información en los registros. Esta normativa solo aplica a las agencias federales, no abarca a las empresas privadas. Sin embargo, constituye un buen comienzo con respecto a la protección de datos personales, pero es insuficiente.

Exige que el tratamiento de la información personal esté justificado y sea relevante para el ejercicio de las funciones propias del órgano y para la consecución de la finalidad perseguida, debiéndose contar con el consentimiento del titular para su revelación a terceros, salvo las excepciones que prevé la norma, reconociéndose el derecho de acceso y rectificación, así como el derecho a interponer recursos y acciones ante su incumplimiento.

c) **Family Educational Rights and Privacy Act (FERPA) of 1974[221].**

Esta normativa también es conocida como Enmienda Buckley. La FERPA incorpora el concepto de protección a la confidencialidad de la información académica de los estudiantes (desde nivel elemental hasta el universitario). Provee los mecanismos para hacer valer estos derechos de privacidad y las excepciones correspondientes, así como los procesos de acceso y revisión de los estudiantes a

---

[220] Privacy Act (PA) of 1974, U.S.C. 5 § 552a, [en línea], http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf

[221] Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g, [en línea], https://www.law.cornell.edu/uscode/text/20/1232g

su información académica y personal. Su cumplimiento es obligatorio para todas las instituciones que reciben fondos federales directos e indirectos.

d) **Right to Financial Privacy Act (RFPA) of 1978[222].**

Esta norma obliga emitir una orden judicial para acceder a los registros financieros de las personas cuando son requeridos por las autoridades gubernamentales.

e) **Foreign Surveillance Act (FISA) of 1978[223].**

Esta permite la vigilancia de comunicaciones electrónicas de los extranjeros, las cuales no requieren de una orden judicial, pero necesita la autorización de la Procuraduría General. Además, mediante esta ley se creó un Tribunal para estudiar las peticiones de órdenes secretas de vigilancia interna.

En el año 2001, luego de los ataques terroristas contra los EE.UU., la ley FISA, toma relevancia luego de la aprobación de la Ley Patriota USA-Patriot Act[224], mediante la cual se ampliaron las capacidades de vigilancia de este gobiernos.

---

[222] Right to Financial Privacy Act (RFPA) of 1978, 12 U.S. Code Chapter 35, [en línea], https://www.law.cornell.edu/uscode/text/12/chapter-35

[223] Foreign Surveillance Act (FISA) of 1978, 50 U.S. Code Chapter 36, [en línea], https://www.law.cornell.edu/uscode/text/50/chapter-36

[224] USA-PATRIOT Act (USAPA) of 2001, Pub. L. No. 107-56, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

f) **Privacy Protection Act (PPA) of 1980[225].**

En principio esta normativa limita las capacidades de las agencias del gobierno para confiscar y buscar la información producto de la prensa y los medios.

g) **Cable Communications Policy Act (CCPA) of 1984[226].**

Esta normativa exige a los operadores de cable informar a los suscriptores sobre la naturaleza y usos de la información personal recopilada. Asimismo, prohíbe a estas empresas revelar la información de hábitos de consumo o visualización de las personas, también protege a los consumidores con una *private cause of action* (acción legal privada) para demandar la protección de este derecho. Esta ley solo es aplicable a los operadores de cable y tiene amplias excepciones para revelar información a causa de una actividad comercial legítima. A pesar de lo anterior, la CCPA es un paso importante en la protección de datos personales, al permitir a los consumidores el control sobre sus registros de cable.

h) **Electronic Communications Privacy Act (ECPA) of 1986[227].**

El Congreso de los EE.UU. modernizó las leyes sobre la vigilancia electrónica con la aprobación de la ECPA. En esta normativa se amplían las protecciones contenidas en la Ley federal de escuchas telefónicas de 1968, ampliando el contenido a la comunicación de datos, video, teléfonos móviles y correo electrónico.

---

[225] Privacy Protection Act (PPA) of 1980, 42 U.S. Code Chapter 21ª, [en línea], https://www.law.cornell.edu/uscode/text/42/chapter-21A

[226] Cable Communications Policy Act (CCPA) of 1984, 47 U.S.C. § 551, [en línea], http://www.publicaccess.org/cableact.html

[227] Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. § 2510-22, [en línea], https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

Esta normativa restringe la interceptación de comunicaciones transmitidas y búsqueda de comunicaciones almacenadas.

i) **Computer Matching and Privacy Protection Act (CMPP) of 1988[228].**

La norma regula las investigaciones automatizadas conducidas por parte de las agencias de gobierno relacionadas con la comparación de archivos de computadora.

j) **Employee Polygraph Protection Act (EPPA) of 1988[229].**

Esta normativa prohíbe a los empleadores someter al "detector de mentiras" o polígrafo a los empleados o futuros empleados. No aplica para los empleados gubernamentales o para asuntos de seguridad nacional.

k) **Video Privacy Protection Act (VPPA) of 1988[230].**

Esta ley también es conocida como *the Bork Bill.* En principio prohíbe a los proveedores de servicios de video la divulgación de los títulos que compran o alquilan las personas. Sin embargo, esta ley solo aplica a las tiendas de videos y no existen restricciones para las librerías, estudios de grabación o cualquier otro tipo de distribuidor, productores de revistas o ventas por catálogo.

---

[228] Computer Matching and Privacy Protection Act (CMPP) of 1988, 5 U.S. Code § 552ª, [en línea], https://www.law.cornell.edu/uscode/text/5/552a

[229] Employee Polygraph Protection Act (EPPA) of 1988, 29 U.S. Code Chapter 22, [en línea], https://www.law.cornell.edu/uscode/text/29/chapter-22

[230] Video Privacy Protection Act (VPPA) of 1988, 18 U.S.C. §§ 2710-11, [en línea], https://www.law.cornell.edu/uscode/text/18/2710

l) **Telephone Consumer Protection Act (TCPA) of 1991[231].**

Esta normativa incluye la protección para demandar a quienes ofrecen productos o servicios vía telefónica y establece multas de quinientos dólares estadounidenses a quienes sigan llamando luego de haber solicitado no ser llamado de nuevo. Esta normativa protege contra las molestias telefónicas, pero, no regula la recopilación de datos o la venta de estos.

m) **Driver's Privacy Protection Act (DPPA) of 1994[232].**

Esta regulación constituye un importante avance con relación a la información personal revelada por parte del gobierno a la industria, pero, solo aplica para la información relacionada con el registro de vehículos y no a todos los demás registros que tiene el Estado en su poder. Mediante esta normativa se prohíbe la utilización de la información obtenida del registro estatal de vehículos automotores.

n) **Health Insurance Portability and Accountability Act (HIPAA) of 1996[233].**

Esta ley regula sobre los registros médicos en posesión del Departamento de Salud y Servicios Humanos. Esta información requiere autorización para todos los usos con algunas excepciones relacionadas con el tratamiento, pago de servicios y la salud de las personas.

---

[231] Telephone Consumer Protection Act (TCPA) of 1991, 47 U.S.C. § 227, [en línea], https://transition.fcc.gov/cgb/policy/TCPA-Rules.pdf

[232] Driver's Privacy Protection Act (DPPA) of 1994, 18 U.S. Code Chapter 123, [en línea], https://www.law.cornell.edu/uscode/text/18/part-I/chapter-123

[233] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 [en línea], http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf

o) **Identity Theft and Assumption Deterrence Act (ITADA) of 1996[234].**

Esta normativa está relacionada con los fraudes cometidos con documentos de identidad de las personas. Sanciona la transferencia o uso fraudulentos de identificaciones con la intención de cometer un delito.

p) **Children's Online Privacy Protection Act (COPPA) of 1998[235].**

Esta es la primera ley en abordar la privacidad en Internet. Regula y protege los datos personales de los menores de edad en Internet. Algunas páginas web deben obtener el consentimiento informado por parte de los padres de los menores, pero su alcance es limitado puesto que solo aplica a los sitios web cuanto estos tienen conocimiento efectivo de que se están recogiendo datos personales de jóvenes menores de 13 años de edad. Esta ley no protege a los internautas mayores de 13 años.

q) **Gramm-Leach-Bliley (GLB) Act of 1999[236].**

Esta normativa permite a las empresas financieras compartir datos personales no públicos, con otras empresas afiliadas, sin embargo, las personas pueden optar por no permitir que esta información sea compartida con terceros. En

---

[234] Identity Theft and Assumption Deterrence Act (ITADA) of 1996, 18 U.S. § 1028, [en línea], https://www.law.cornell.edu/uscode/text/18/part-I/chapter-47

[235] Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. § 6501–6505, [en línea], https://www.law.cornell.edu/uscode/text/15/chapter-91

[236] Gramm-Leach-Bliley (GLB) Act of 1999, 12 U.S.C. § 1811, [en línea], https://www.law.cornell.edu/uscode/text/12/1811

la práctica, la GLB facilita la divulgación de datos personales. Una de las críticas que recibe es que las empresas financieras no brindan suficiente información a las personas sobre las políticas de privacidad existentes, para que puedan ejercer estos derechos de forma efectiva.

r) **CAN-SPAM Act of 2003[237].**

Esta normativa se refiere a los correos no solicitados (*spam*) o basura, utilizados en el comercio. Se establecen siete principios jurídicos básicos que deben cumplir las empresas. Estas actividades empresariales son vigiladas por la FTC, que ha emitido en el año 2009 una Guía de cumplimiento para las empresas[238].

s) **Fair and Accurate Credit Transactions Act (FACT) of 2003[239].**

Esta normativa regula las transacciones de crédito y desarrolla una sección tendiente a proteger el robo de identidad.

---

[237] CAN-SPAM Act of 2003, Pub. L. No. 108-187, [en línea], https://www.law.cornell.edu/wex/inbox/can-spam_act_core_requirements

[238] CAN-SPAM Act: A Compliance Guide for Business, [en línea], https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

[239] Fair and Accurate Credit Transactions Act (FACT) of 2003, Pub. L. 108-159, [en línea], https://www.law.cornell.edu/cfr/text/16/602.1

t) **Video Voyeurism Prevention Act (VVPA) of 2004[240].**

Regula la intensión o captura de imágenes de área privadas de una persona sin su consentimiento o conocimientos de circunstancias especiales.

De forma general, todas estas leyes de privacidad no suponen una protección efectiva de la privacidad de las personas y sus datos, puesto que constituyen un mosaico de leyes que dejan huecos en muchos supuestos que debería brindarse la protección[241]. Estas normas tienen un problema de efectividad pues existen muchas dificultades para hacerlas cumplir.

u) **Genetic Information Nondiscrimination Act (GINA) of 2007[242].**

Esta es la primera ley federal que prohíbe toda discriminación en base a la información genética en el ámbito de los seguros médicos y del empleo, impidiendo a los empresarios recabar información genética de sus empleados y prohibiendo a las aseguradoras rechazar la cobertura o incrementar las primas basándose en la predisposición genética de una persona a enfermar.

---

[240] Video Voyeurism Prevention Act (VVPA) of 2004, Pub. L. 108–495, [en línea], https://www.law.cornell.edu/uscode/text/18/1801

[241] SOLOVE, D. J., *The digital person. Technology and privacy* …, *op. cit.,* [versión para lector digital Kindle].

[242] Genetic Information Nondiscrimination Act (GINA) of 2007, Pub. L. 110–233, title II, § 201, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/html/PLAW-110publ233.htm

2.1.4.4. Leyes que permiten a las agencias gubernamentales la toma de datos sensibles o facilitan las técnicas de investigación.

Así como existen leyes o estatutos que protegen la privacidad de las personas, se han dictado otras leyes que crean excepciones con respecto a la protección de la privacidad o los datos personales, en ciertas circunstancias especiales, como las siguientes:

a) **Bank Secrecy Act (BSA) of 1970[243].**

Esta norma permite a las agencias gubernamentales, requerir información de transacciones financieras y recibir reportes para el seguimiento de delitos de cuello blanco y para protegerse contra el terrorismo internacional.

b) **Communications Assistance for Law Enforcement Act (CALEA) of 1994[244].**

Esta permite a los tribunales ordenar a proveedores de servicios de comunicaciones el apoyo para la intervención de comunicaciones y la vigilancia. Se prevén multas para los operadores que no colaboren con las autoridades.

---

[243] Bank Secrecy Act (BSA) of 1970, Pub. L. 91–508, [en línea], https://www.law.cornell.edu/uscode/text/31/5311

[244] Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. 103–414, [en línea], https://www.law.cornell.edu/uscode/text/18/2522

c) **Personal Responsibility and Work Opportunity Reconciliation Act (PRWOR) of 1996[245].**

Mediante esta normativa se permite la recolección de información personal de los nuevos trabajadores, como el número de seguridad social, la dirección y salario, registros que serán almacenados en una base de datos nacional.

d) **USA-PATRIOT Act (USAPA) of 2001[246].**

Una ley dictada luego de los atentados terroristas del 9 de setiembre de 2001, que permite procedimientos de vigilancia de cualquier tipo de comunicaciones, orales o escritas, a través de cualquier medio. Por medio esta ley se modifican varias leyes de la citadas anteriormente, que se relacionan con las comunicaciones, como la ECPA y FISA, concediendo amplias facultades a las agencias gubernamentales para combatir el terrorismo a través del acceso a la información y las comunicaciones de las personas. Esta norma tenía una cláusula de extinción (31 de diciembre de 2005) por lo cual fue renovada en marzo de 2006 por parte del Congreso de los EE.UU., fecha en que se realizaron cambios sustantivos para no incurrir en posibles inconstitucionales.[247]

Según Saldaña[248], la USAPA fue aprobada como una ley extensa, con más de ciento cincuenta secciones y enmiendas de más de quince disposiciones legislativas federales, con ello se reforzaron los procedimientos de vigilancia de las

---

[245] Personal Responsibility and Work Opportunity Reconciliation Act (PRWOR) of 1996, Pub. L. 104–193, [en línea], http://www.law.cornell.edu/uscode/text/42/616&prev=search

[246] USA-PATRIOT Act (USAPA) of 2001, Pub. L. No. 107-56, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[247] *Vid.* Capítulo VI, *infra*, sobre la vigilancia masiva.

[248] SALDAÑA, M. N., "La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de información personal en los Estados Unidos", *Revista Aucaria*, vol. 9, num. 18, 2007, pp. 112-113.

comunicaciones, para abatir el blanqueo de dinero internacional y la financiación terrorista, se removieron obstáculos para la investigación terrorista, se endurecieron las normas penales frente al terrorismo internacional, se aumentaron las atribuciones de los cuerpos de seguridad y de los servicios de inteligencia norteamericanos y se amplió la definición de "actividad terrorista" hasta el punto que pudieran ser incluidas actividades no violentas opuestas a la política exterior norteamericana, recordando en sus disposiciones y su espíritu a la conocida *Smith Act* vigente durante los años cincuenta en tiempos de la Guerra Fría, el macartismo y la lucha contra el comunismo en los Estados Unidos.

En el Título II (Secciones 201 a 215) de esta normativa se reforzaron los procedimientos de vigilancia de las comunicaciones y se reforzaron, entre otras, las disposiciones contenidas en la ECPA de 1986. La reforma más importante operada a través de la USAPA ha tenido lugar a través de las modificaciones de la FISA, que había sido aprobada en 1978 para reforzar la protección de los derechos garantizados en la Cuarta Enmienda, se prohibió así el control de las conversaciones telefónicas y las comunicaciones postales y electrónicas sin la correspondiente autorización judicial del Tribunal Federal de Vigilancia de Inteligencia Extranjera establecido *ad hoc* y cuyas actuaciones tienen carácter secreto.

Todas estas reformas afectaron las garantías de protección de la privacidad de la información personal frente a intromisiones ilegítimas del gobierno amparadas por la Cuarta Enmienda, lo cual permitió el acceso, sin necesidad de una orden judicial, de los servicios de inteligencia y el intercambio con otras agencias del gobierno y con gobiernos extranjeros, a información sensible que había sido acumulada en investigaciones criminales recogida de archivos escolares, transacciones financieras, actividad en la red, conversaciones de teléfono, o informaciones derivadas de procedimientos judiciales que no estén incluso directamente relacionadas con casos de "terrorismo".

Asimismo, esta norma admite órdenes judiciales por las que se autorizan los registros secretos de domicilios sin el conocimiento de su titular, *sneak and peek warrant,* y es posible retrasar la comunicación de lo sucedido si se encontrase causa razonable para creer que la notificación tuviese un efecto adverso, así como el espionaje secreto de líneas telefónicas *roving wiretaps*. Igualmente, se ampliaron las medidas de monitoreo electrónico, en las que se incluyeron las direcciones y *routing* de todo el tráfico de Internet, correo electrónico, direcciones IP, y URL's de los portales de Internet, sin la exigencia de mostrar una "causa probable" de conducta criminal, eludiéndose así las garantías de la Cuarta Enmienda.

La abundante normativa aprobada el Congreso de los EE.UU., relacionada con la información personal, de forma fragmentaria contempla numerosas excepciones y adolecen de lagunas importantes. Sin embargo, se cuenta en este país con la protección constitucional *right to informational privacy*. Luego de los actos terroristas del 11 de setiembre de 2001, se han estancado los niveles de protección alcanzados generalizándose la interceptación y utilización de las comunicaciones electrónicas en razón de la protección de la seguridad nacional.

2.1.4.5. The Federal Trade Commission (FTC).

La Comisión Federal de Comercio fue creada en 1914, cuando el presidente Woodrow Wilson firmó la Ley de la FTC, siendo su misión principal, proteger a los consumidores y promover la competencia[249]. La FTC no tiene las potestades de intervenir en conflictos particulares o específicos; sin embargo, puede tomar

[249] Acerca de la FTC, https://www.ftc.gov/about-ftc/our-history

medidas contra una empresa contra la cual se han recibido varias denuncias por parte de los consumidores[250].

Esta Comisión fue creada por el Congreso de EE.UU. y está dirigida por cinco comisionados nombrados. Se separa en dos oficinas diferentes: la oficina de protección del consumidor, que se centra en los fraudes a consumidores y publicidad engañosa; y, la oficina de competencia, que se ocupa de la defensa de la libre competencia.

Con respecto a las políticas de privacidad, la FTC ha interpretado que la ley no permite los actos o prácticas injustas o engañosas que afecten al comercio. Para ello tiene la facultad de tomar acciones civiles y buscar remedios a través de mandatos judiciales o medidas cautelares[251].

Solove y Hartzog[252] sostienen que la jurisprudencia de la FTC, sobre la privacidad, es en la práctica el equivalente a un cuerpo de derecho común. Ambos autores sostienen que la jurisprudencia de esta Comisión es tan importante que podría desarrollar las bases de una "ley común" en el tema de la privacidad.

Tal y como se ha expuesto, la regulación de la privacidad en los EE.UU. se encuentra fragmentada, constituida en esencia por estatutos y los *privacy torts law.* Estas regulaciones resultan un tanto difusas como discordantes y en definitiva no bastan para proteger todos los agravios contra la privacidad que suelen darse, tanto

---

[250] En la práctica, la jurisprudencia sobre privacidad de la FTC se ha convertido en la fuerza más amplia y de mayor influencia reguladora sobre información privada en los EE.UU., más que cualquier estatuto de privacidad o cualquier agravio derecho común. SOLOVE, D. J. y HARTZOG, W., "The FTC and the New Common Law of Privacy", en 114 *Columbia Law Review* 583 (2014), GWU *Legal Studies Research Paper* No. 2013-120, GWU *Law School Public Law Research Paper* No. 2013-120, Agosto, 2013, [en línea], http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913

[251] SOLOVE, D. J. y HARTZOG, W., "The FTC and the New Common Law of Privacy", *op. cit.,* [en línea].

[252] *Ibíd*.

por parte de las agencias gubernamentales como por parte de las empresas privadas.

Del apartado anterior se podría recordar que existe una ley para la protección de los registros de video y otra diferente para la protección de los registros de cable, así como otras que protegen la información personal de los menores de 13 años; sin embargo, se echa de menos una ley común federal que proteja la privacidad de los datos recogidos por parte del comercio electrónico.

Muchas de las grandes empresas comerciales cuentan, en la actualidad, con políticas de privacidad, trabajo que ha sido reconocido a la FTC[253]. En sus funciones, la FTC puede imponer sanciones a las empresas infractoras de las políticas de privacidad, por lo cual las empresas que han quedado fuera de las regulaciones estatales encuentran en la FTC una fuente primaria para la regulación sobre la privacidad de la información de las personas.

En el marco de las regulaciones de la privacidad aparece este "cuerpo legal" que aún no ha sido analizado por los especialistas en derecho a la privacidad, ni siquiera se ha catalogado entre la taxonomía de la ley, por lo cual es difícil dar un lugar a estas regulaciones que se han propagado en la práctica a través de los contratos privados como políticas de privacidad[254].

Los autores citados estiman que el auge de las políticas de privacidad utilizadas en los contratos, se debe al fracaso de la protección que ofrecían los

---

[253] SCHNEIER, B., *Data and Goliath. The hidden battles to collect your data and control your world,* Editorial W.W. Norton & Company, New York, London, 2015, [versión para lector digital Kindle].

[254] SOLOVE, D. J. y HARTZOG, W., "The FTC and the New Common Law of Privacy", *op. cit.,* [en línea].

agravios civiles (*torts law*) para proteger la privacidad de las personas[255], principalmente, para proteger los datos en línea.

Ciertamente, uno de los primeros mecanismos legales en el uso de tecnologías en línea, fue la autorregulación, sin embargo, ha parecido un fracaso, sobre todo luego de las denuncias realizadas por Snowden, al revelar que las empresas dedicadas al uso de tecnologías suministran la información de los usuarios a las agencias del gobierno de los EE.UU.

A inicios de los años noventa, cuanto iniciaba la popularidad de Internet, las personas eran reacias a colocar sus datos en línea ante el posible riesgo del uso no autorizado de sus datos. Ante ello, las empresas tuvieron que ajustar la seguridad en línea para motivar la utilización de estos servicios. Empresas como TRUSTe[256] iniciaron con certificados para garantizar la seguridad de las páginas web, incluso hoy día es frecuente que al entrar a una página de pago se utilicen servicios de seguridad contratados a terceros.

Las políticas de privacidad por lo general son incluidas en los contratos, sin embargo, existe la duda si forman parte de este, las cuales, en principio, permiten a las partes el reclamo por daños contractuales relacionados con violaciones a las políticas de privacidad. Pareciera razonable incluir cláusulas contractuales sobre la privacidad de datos personales, pero en la práctica esto ha resultado lejos de ser

---

[255] *Ibíd.*

[256] Esta empresa se proyecta como líder mundial en la privacidad de los datos de las empresas, para que estas puedan utilizar esos datos de forma segura entre las distintas partes comerciales (clientes, empleados, proveedores, transportistas, etc.). https://www.truste.com/

efectivo[257]. Existen muchos obstáculos para el reclamo de incumplimientos contractuales sobre las cláusulas de privacidad, litigios complicados, jurisdicciones lejanas, cláusulas abusivas y otros, puesto que se trata de una jurisdicción especializada para el litigio de negocios, cuando lo que se requiere, en realidad, es la protección del derecho a la privacidad de las personas.

En la actualidad la mayoría de páginas y servicios en la web ofrecen políticas de privacidad en forma de contratos, sin embargo, no hay muchos precedentes jurisprudenciales sobre reclamaciones por la violación de estas políticas de privacidad[258].

Aunque la mayoría de los procesos judiciales, en los cuales se han reclamado violaciones a las políticas de privacidad, se han desestimado, se ha reconocido la posibilidad, por parte de algunos tribunales[259], de poder reclamar estos derechos en esa vía. El derecho contractual, pareciera, ha jugado un papel marginal a efectos de resolver las disputas sobre posibles violaciones de las políticas de privacidad incluidas en los contratos.

En la actualidad, la FTC es vista como la agencia federal de hecho para la protección de datos. La ley de la FTC solo puede ser aplicada a las violaciones que ahí se contemplan y carece de la potestad de promulgar normativa o sus propias reglas, sin embargo, con anterioridad a las intervenciones de la FTC, la mayoría de las empresas no incluían políticas de privacidad en sus contratos.

---

[257] SOLOVE, D. J. y HARTZOG, W., "The FTC and the New Common Law of Privacy", *op. cit.,* [en línea].

[258] Al efecto, se pueden consultar algunos precedentes jurisprudenciales en los cuales se discuten entre los agravios, violaciones a las cláusulas de privacidad, Daniels v. JP Morgan Chase Bank, NA, No. 22575/09, 2011; Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 864–65, ND Cal. 2011; Loeffler v. Ritz-Carlton Hotel Co., No. 2:06-CV-0333-ECR-LRL.

[259] *Vid.* Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 864–65, ND Cal. 2011.

En materia de protección de datos, la FTC adquirió tanta importancia debido a dos razones principales: a) por la ampliación de la jurisdicción, dado que en 1998, el Congreso de los EE.UU. le atribuyó funciones particulares para la protección de datos a través de la Ley COPPA; b) debido a que el marco de aplicación de la FTC era compatible con el modelo de autorregulación instaurado políticamente.

2.2. Teorías del derecho de intimidad.

Existen varias teorías sobre la protección del derecho de intimidad, la teoría de las esferas o círculos concéntricos desarrollada por Hubman, la teoría del mosaico desarrollada por Madrid Conesa y la teoría del "*right to privacy*" desarrollada por William Prosser.

Todas estas teorías ponen de relieve la tutela de la intimidad y la privacidad desde diversas posiciones, resulta esencial es estudio de cada una de ellas puesto que dependiente de los agravios que enfrenta la intimidad cada uno podría aportar una forma distinta de protección. De esta manera, las teorías de protección de estos derechos podrían plantearse como solución frente a las diversas vulneraciones que en la actualidad enfrentan las personas al desarrollo de sus vidas privadas. Con el propósito de sistematizar y hacer un recuento de las teorías de la privacidad, se expone cada una de ellas.

2.2.1. Teoría Sphärentheorie (Teoría de las esferas o círculos concéntricos).

Esta teoría fue desarrolla por Hubman, quien divide el contenido de la intimidad en tres grandes esferas[260], la primera de ellas, se conforma por el círculo más amplio o esfera privada, que abarca todos los comportamientos, noticias y expresiones que la persona no desea que sean de conocimiento público y se le denomina, *privatsphäre*; la otra se refiere a lo confidencial, *vertravensphäre, y;* la última de estas, se conforma con lo secreto, *gehimsphäre.* En términos generales se distinguen ámbitos de acción del individuo, de extensión radial, a modo de círculos concéntricos, cuyo centro más cercano corresponde a lo secreto, su periferia a aquello que atañe a la individualidad de la persona, y una franja

[260] LÓPEZ DÍAS, E., *op. cit.,* pp. 197-198. *V. et.* REBOLLO DELGADO, L., *op. cit.*, pp. 140 y ss.

intermedia correspondiente a la intimidad, en que se sitúa aquello que se desea mantener al margen de la injerencia de terceros.

2.2.1.1. Privatsphäre:

Es la esfera privada amplia, la que comprende todos aquellos comportamientos, noticias y expresiones que el sujeto desea que lleguen a conocimiento público.

2.2.1.2. Vertravensphäre:

Es la esfera confidencial que abarca lo que el sujeto comunica a otra persona de su confianza. Aquí se excluye al público general, y a aquellas personas que operan en la vida privada y familiar.

2.2.1.3. Gehimsphäre:

Es la esfera o círculo menor de lo secreto que corresponde a las noticias y hechos que por su carácter reservado, no pueden ser accesados por los demás.

Estas esferas se comunican entre sí y se conforman libremente por cada individuo atendiendo a sus propias pretensiones, su estrato social o su popularidad. Así se protege la dignidad del individuo y se configura el derecho a la intimidad como un derecho de defensa.

2.2.2. Teoría del Mosaico.

Esta teoría es desarrollada por Madrid Conesa[261], quien criticaba el carácter absoluto y separatista de la Teoría de las Esferas. Esta segunda teoría considera a lo público y lo privado como conceptos relativos, en función de quien sea el otro

[261] MADRID CONESA, F., *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984, pp. 45.

sujeto en la relación informativa. Asimismo, parte de la idea de que existen datos que a priori son irrelevantes, desde el punto de vista del derecho a la intimidad y que, sin embargo, en conexión con otros, también pueden servir para hacer totalmente transparente la personalidad de un ciudadano, al igual que ocurre con las pequeñas piedras que forman un mosaico, que en sí no dice nada, pero que unidas pueden formar en su conjunto plenos significados.

Esta teoría surge como contrapartida a la teoría de las esferas o de los círculos concéntricos, en la que los alemanes distinguían que el núcleo interior de las esferas lo constituía lo íntimo –lo inobservable-, en una más externa lo familiar o privado -lo posiblemente observable-, en otra lo secreto y confidencial, siendo la última, la esfera de lo público -lo necesariamente observable-.

2.2.3. Teoría del "right to privacy".

La teoría del "right to privacy" fue desarrollada en el año 1960 por William Prosser[262], quien divide el concepto unitario de privacidad, en cuatro situaciones distintas de violación: a) Intrusión en la soledad de la vida de una persona o en sus asuntos privados. b) Divulgación de hechos embarazosos que afectan a la persona. c) Publicidad que podría desprestigiar a la persona ante la opinión pública. d)

[262] PROSER, W. L., "Privacy", *California Law Review,* vol. 48, No. 3, 1960, p. 389, [en línea], http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview. A William Prosser se le ha reconocido como el gran creador del derecho estadounidense moderno sobre delitos contra la privacidad, su teoría replicó en la doctrina de la época, como ilustre e influyente en el tema de intimidad informática o "privacy". El nombre de William Lloyd PROSSER, Decano de la Facultad de Derecho de Universidad de Berkeley (1948-1961), en 1960 hizo historia con la publicación citada.

Apropiación (con ventaja de la otra parte) del nombre o del aspecto físico del afectado[263].

Tanto el artículo "*The Right to Privacy*" de Warren y Brandeis, como "*Privacy"* de Prosser, así como la jurisprudencia de la Suprema Corte de los Estados Unidos de Norteamérica, han significado un paso trascendental para el reconocimiento del derecho de intimidad. Los aportes realizados tienen un incalculable valor para la época actual y la evolución de este derecho, lo cual se puede sintetizar en cuatro áreas: 1. Libertad o seguridad frente a cualquier tipo de intromisiones indebidas en la esfera privada; 2. Garantía de respeto a las opiniones personales en materia de asociación o creencias; 3. Tutela de la libertad de elección sin interferencias; y 4. Posibilidad de los individuos o grupos de acceder y controlar las informaciones que les atañen[264].

---

[263] La teoría de Prosser desarticulaba el "general right to privacy" de Brandeis. Después de los proyectos presentados ante la Cámara de los Lores en Inglaterra de Lord Mancroft, de Lyon (1967), de Brian Walden (1969), de Kenneth Baker (1969), de Leslie Huckfield (Control of personal information, 1971), aparece el informe de Kenneth Younger "Younger Report" (1972). El "Younger Committee" consideraba que el concepto de privacy no podía ser definido de manera satisfactoria, a la vez que disentía de la conceptualización de la privacy como el derecho a ser dejado solo *"right to be let alone"*.

[264] Westin define la privacidad como *"el derecho al control de la información referente a uno mismo"; o "el derecho de los individuos, grupos o instituciones a determinar por sí mismos, cuando, cómo y hasta qué punto se puede comunicar a terceras personas información referida a ellos"*, WESTIN, A., "Privacy and freedom", *Administrative Law Review,* vol. 22, No. 1, octubre 1969 [en línea], http://www.jstor.org/stable/40708684.

2.3. Características.

El derecho de intimidad al estar catalogado como un derecho personalísimo, le son aplicables las características esenciales que componen estos derechos. Santos Cifuentes[265] expone tales características las cuales se comentan a continuación:

2.3.1. Derecho Innato.

Desde una perspectiva iusnaturalista, el derecho de intimidad sería innato, es decir, depende de la existencia de un sujeto, el principio existencial coincide con el de la persona misma. No es necesaria formalidad alguna para la existencia. Si este derecho fuese reconocido con posterioridad a la existencia de la persona, sería un derecho adquirido.

Esta característica conlleva a que se trata de un derecho inherente a la condición humana, que nace con el sujeto, es consustancial a él, no es necesario requisito o condición alguna para su ejercicio[266].

La síntesis de esa característica, al igual que los derechos personalísimos, la constituye el hecho de estar adherido a la existencia misma de la persona, nacen y se extinguen en sincronía con los seres humanos, lo que se explica en la siguiente de las características.

---

[265] CIFUENTES, S., *op. cit.,* pp. 23-26. *Cfr.* CIFUENTES, Santos, *Derechos personalísimos,* Astrea, Buenos Aires, 1995, p. 175.

[266] En palabras de Santos Cifuentes, la connaturalidad relevante deriva, filosóficamente hablando, del primer momento de la existencia del derecho. Si este aparece automáticamente con el principio de la persona, porque normativamente se lo tutela, desde entonces, puede decirse que es innato, CIFUENTES, S., *op. cit.,* p. 23.

2.3.2. Derecho vitalicio e inherente.

El derecho de intimidad permanece durante toda la vida de la persona y se extingue con su muerte. Tiene una duración *ad vitam*, para toda la vida del titular y es intransmisible a los herederos.

Es importante advertir que el derecho a la honra o el honor de una persona es transmisible a los herederos, sin embargo, la naturaleza de ese derecho cambia al producirse esa transmisión, pues se trata de un derecho *post mortem,* el cual podría ser reclamado por quienes tengan legitimación para esto. La tutela jurídica de ese derecho y la forma de ejercitarla debe ser en procesos de tutela distintos.

El buen nombre o reputación de una persona podría ser defendido por los herederos, pero tal y como se advirtió no se trata de la transmisión del derecho de intimidad a estos.

La protección legal de este derecho, luego del fallecimiento de la persona, ocurre fuera del ámbito de protección de los derechos fundamentales.

2.3.3. Derecho Esencial.

Se había adelantado que la privacidad no es un derecho eventual, es decir, no es un derecho derivado o adquirido, pues no depende de circunstancias distintas de la mera existencia de la persona.

Este derecho personalísimo, presenta una importancia mayor a cualquiera de los otros, pues está claro que no es de carácter eventual, no deriva de circunstancias ajenas al principio de existencia de la persona; por tanto, no es un

derecho derivado o adquirido[267]. Su carácter esencial deriva de esa importancia para nuestra condición humana. El reducto de privacidad obligatoriamente respetado por terceros resulta vital, pues "…de nada valdría ser o no propietario, tener o no hijos y ejercer la patria potestad, poder o no trabajar, si se careciera de un centro equilibrador y respetado de la vida sola o de lo íntimo del sujeto. Si este todo lo debiera comunicar o si los demás pudieran avasallar ese reducto infaltable"[268]. Puede interpretarse entonces que, junto con la vida, la intimidad es uno de los derechos fundamentales en el desarrollo de la dignidad humana.

2.3.4. Necesario.

Se estima que la intimidad tiene una función constitutiva de la persona misma. Para Santos Cifuentes, *"…no podrían crearse los productos del espíritu si solo fuera posible transcurrir con la subsistencia fatalmente hacia afuera, o sea con una inevitable exteriorización mundana; desaparecería la inspiración creativa si faltara la posibilidad de tener un reducto interior y sin que parciales sectores de la comunicación quedaren reservados a pocos y determinados sujetos del entorno común; si fuera imposible algún misterio del yo frente a la colectividad abstracta y*

[267] El carácter personalísimo de estos derechos ha sido subrayado por el Tribunal Constitucional Español (caso Pantoja-Paquirri, STC 231/88), al declarar que su disfrute finaliza, al menos en cuanto a su dimensión constitucional, con la vida del propio individuo. Aunque el legislador puede ampliar su protección más allá de la vida del sujeto afectado (como efectivamente se hace en la ley 1/82, de 5 de mayo, otorgando acción indemnizatoria por intromisiones ilegítimas a los familiares del fallecido e, incluso, al Ministerio Fiscal), tal protección civil post mortem ocurre, en palabras del Tribunal Constitucional, "fuera del área de protección de los derechos fundamentales que se encomienda al Tribunal Constitucional mediante el recurso de amparo". *En* LÓPEZ GUERRA, L., *et.ál.*, *op. cit.,* [versión para lector digital Kindle].

[268] CIFUENTES, S., *op. cit.,* p. 24.

general; aluna privacidad preservada del saber de todos los congéneres que popularmente nos rodean"[269].

2.3.5. De objeto interior.

Se refiere a una prerrogativa jurídica inseparable del hombre en sí. El objeto y el sujeto son inseparables, no existiría el objeto sin esa relación o enlace con el sujeto, circunstancia inseparable entre ambos.

2.3.6. Temporalmente disponible.

Puede decirse que este derecho, aunque fuera del comercio e intransferible, resulta temporalmente disponible. Pueden entregarse o cederse a los demás parcelas definidas de información, concretas y por un tiempo corto[270].

Pese a la anterior posibilidad, debe entenderse que la enajenación o renuncia total y absoluta importaría un sometimiento inaceptable de la persona a la sociedad o a los otros individuos que la integran[271].

2.3.7. Extrapatrimonial.

Este derecho no puede catalogarse dentro de la gama de derechos patrimoniales, los cuales son posibles de tasar económicamente. Tampoco, significa que, en caso de ser vulnerado, no sea motivo de resarcimiento, a manera de compensación por sacrificio especial o daño producido por la Administración Pública o un particular. Puede aquí incluirse lo especial que resulta a este derecho

---

[269] CIFUENTES, S., *op. cit.,* pp. 12 y 24.

[270] CIFUENTES, S., *op. cit.,* p. 25.

[271] El Tribunal Constitucional ha indicado, en diversas ocasiones, que cada individuo puede renunciar temporalmente a su ejercicio o disfrute. *Cfr.* LÓPEZ GUERRA, L., *et.ál.*, *op. cit.,* [versión para lector digital Kindle].

la valoración en cuanto al daño moral, sea este subjetivo, como la afectación interna del sujeto o como daño moral objetivo, entendido como el causado con efecto externo como la imagen o el honor que, eventualmente, hasta pueden producir daños económicos a quien lo sufre. Así, aunque no patrimonial, el desconocimiento o violación de este derecho sí puede generar responsabilidades de tipo patrimonial.

Los bienes sobre los que recae este derecho no son de índole patrimonial, están fuera del comercio y como se indicó ello no es obstáculo para que se puedan valorar los daños de forma económica[272].

2.3.8. Absoluto.

La característica más importante del derecho a la intimidad lo constituye la posibilidad de enfrentar a su titular con todas las demás personas, como un "poder jurídico de exclusión"[273].

Debe tenerse claro que, no resulta absoluto este derecho simplemente por su contenido, pues debe, también, respetar la moral, el orden público y, por supuesto, debe observar el derecho ajeno, así como el interés público. Resulta absoluto por ser de exclusión, con similar estructura a los vínculos del derecho real de dominio y, sin embargo, lo dicho, al igual que otros derechos fundamentales no puede considerarse a ultranza como irrestricto.

2.3.9. Autónomo.

Esta característica resulta de cardinal importancia para los efectos de la presente investigación, pues las anteriores características expuestas lo colocan

---

[272] El consentimiento expreso del titular es permitido para la celebración de contratos para comercializar aspectos de la vida íntima, sin embargo, se refiere a algunos aspectos de la intimidad por un período determinado, dado que se trata de un derecho irrenunciable.

[273] CIFUENTES, S., *op. cit.,* pp. 25-26.

como un derecho con una figura jurídica inconfundible. No pueden existir otros derechos que compartan su estructura y modos de ser, pese a la enorme similitud y relación que va a encontrarse con el derecho a la Autodeterminación Informativa, lo cierto es que como se verá, este último también presenta características muy propias y no aplicables al derecho a la intimidad.

2.3.10. Derecho privado.

El derecho de intimidad no podría ser considerado un derecho subjetivo público por cuento se refiere a un derecho subjetivo privado. El goce del derecho y la reacción que pueda ponerse en marcha para su tutela, es ajeno a la consecuencia penal de los actos violatorios. Ese enfoque descarta, además, las interferencias del Estado como colectividad organizada, pues por ser personalísimo es derecho de la persona frente a las otras personas particulares[274].

[274] CIFUENTES, S., *op. cit.,* p. 26.

3. INVIOLABILIDAD DEL DOMICILIO.

Como se ha indicado, el derecho de intimidad protege el conjunto de hechos y situaciones de la vida privada de las personas, lo cual incluye la protección a la vida familiar y su domicilio, por ser este último en el lugar en el cual se desarrolla la mayor parte de la vida familiar.

El derecho a la inviolabilidad del domicilio es una garantía que ha evolucionado, dado que en un principio se entendía en el sentido que no se podía aprehender a un ciudadano sin orden de un juez. En la actualidad debemos entenderlo como una garantía de la vida privada del individuo y, desde luego, se han dado matices con relación a las excepciones.

La Constitución Española incluye la inviolabilidad del domicilio dentro del conjunto de derechos protegidos en el artículo 18, y este constituye la imposibilidad de entrada o registro del mismo salvo en los supuestos tasados por la propia Constitución[275]. Dicha prohibición de entrada y registro afecta, como es evidente, tanto a los agentes de los poderes públicos como a particulares, aunque es la entrada de agentes del poder público el objetivo primordial de la garantía constitucional.[276]

El artículo 18.2 CE, señala lo siguiente:

"El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin el consentimiento del titular o resolución judicial, salvo los casos de flagrante delito".

---

[275] Este derecho puede ser suspendido en los términos previstos mediante ley orgánica, a título individual y con la necesaria intervención judicial y el adecuado control parlamentario, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas según se dispone en el numeral 55.2 de la CE.

[276] LÓPEZ GUERRA, L., *et.ál.*, *op. cit.,* [versión para lector digital Kindle].

En el artículo 23 de la Constitución Costarricense, se indica:

“El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley.”

Si bien es claro que el domicilio es inviolable, deben considerarse ciertos matices con respecto a la definición del domicilio y, para el caso de Costa Rica, determinar, además, que se debe entender por “*todo otro recinto privado”* dado que pareciera una ampliación del término.

Debe advertirse que el concepto de domicilio es distinto desde el área constitucional, civil, penal, comercial, administrativo; tal divergencia debe considerarse a efecto de tener un concepto adecuado para el tema a tratar.

3.1. Concepto de domicilio.

Si bien el domicilio se refiere al lugar de residencia habitual y sede de la persona a efectos jurídicos[277], la inviolabilidad del domicilio se trata más bien de una tutela de carácter instrumental que defiende los ámbitos en que se desarrolla o puede desarrollarse la vida privada de la persona. Ahora bien, ¿puede ser cualquier lugar o requiere de características especiales?, ¿se refiere a la casa de habitación?, ¿al domicilio legal?, ¿la residencia habitual? o ¿simplemente al lugar dónde se encuentre en cierto momento?

El artículo 40 del Código Civil Español define el domicilio de las personas naturales como el lugar de residencia habitual y, en su caso, el que ordene la Ley de Enjuiciamiento Civil[278]. Debe entenderse que el concepto de residencia habitual no exige el transcurso del tiempo, y se refiere a la voluntad de la persona de residir en un lugar determinado, esa voluntad deber ser exteriorizada.

En el caso costarricense, el art. 60 del Código Civil señala que el domicilio real de una persona física es el lugar donde ha establecido la sede principal de sus negocios e intereses. A falta de este, el lugar donde se halle[279].

---

[277] Diccionario Jurídico ESPASA, Madrid, 2001, p. 611.

[278] Código Civil Español, art. 40. *"Para el ejercicio de los derechos y el cumplimiento de las obligaciones civiles, el domicilio de las personas naturales es el lugar de su residencia habitual, y, en su caso, el que determine la Ley de Enjuiciamiento Civil. El domicilio de los diplomáticos residentes por razón de su cargo en el extranjero, que gocen del derecho de extraterritorialidad, será el último que hubieren tenido en territorio español.",* [en línea], https://www.boe.es/buscar/act.php?id=BOE-A-1889-4763

[279] A efectos de que las personas físicas puedan realizar un cambio de domicilio, el artículo 62 del Código Civil de Costa Rica señala que ese cambio se efectúa por el traslado a otro lugar con la intención de fijar allí la sede de sus negocios o intereses.

El concepto o idea de domicilio utilizado en la materia civil, no parece coincidir con el utilizado en el derecho constitucional. La Sala Constitucional ha señalado que "*no puede considerarse domicilio –desde el punto de vista constitucional– a todo espacio en el que pueda desarrollarse la vida privada de la persona, ya que el concepto hace referencia sobre todo al espacio utilizable como residencia"*[280], ligando el domicilio con el desarrollo de la vida privada de la persona, el lugar donde habita, más allá del lugar en el cual la persona desarrolla sus negocios o intereses.

Podría concluirse que a efectos de la tutela constitucional en el caso costarricense el domicilio debe ser considerado como el lugar de residencia en el cual las personas desarrollan su vida privada, limitando el contenido señalado por el constituyente al indicar el domicilio "*todo otro recinto privado"*, pues se interpretó que se refería a los lugares en los cuales sería viable que una persona pueda establecer su residencia.

[280] SSC número 08-9690 de las 15:12 hrs. del 30 de julio de 2008.

3.2. Excepciones.

La Constitución Española contempla tres excepciones al principio de inviolabilidad del domicilio:

a. **Consentimiento:** El consentimiento del titular para que ingresen a su domicilio, lo cual constituye una esta renuncia en una situación determinada y puntual al derecho de intimidad.
b. **Orden judicial:** La decisión de un juez que autoriza el ingreso al domicilio, el cual solo podrá ordenarla mediante un auto motivado cuando existan razones fundadas.
c. **Delito en flagrancia:** Se refiere a los supuestos en los cuales se autoriza el ingreso al domicilio cuando se esté ejecutando un hecho delictivo.

El Tribunal Constitucional Español ha señalado que no es posible aceptar más excepciones que las señaladas en la Constitución. La Ley Orgánica 1/1992, de 21 de febrero, de la Protección de la Seguridad Ciudadana, establecía un supuesto más amparándose en los casos de flagrancia. En el artículo 21.2, señalaba que *"será causa legítima para la entrada en domicilio por el delito flagrante el conocimiento fundado por parte de las Fuerzas y Cuerpos de Seguridad que les lleve a la constancia de que se está cometiendo o se acaba de cometer alguno de los delitos que, en materia de drogas tóxicas, estupefacientes o sustancias psicotrópicas, castiga el Código Penal, siempre que la urgente intervención de los agentes sea necesaria para impedir la consumación del delito, la huida del delincuente o la desaparición de los efectos o instrumento del delito"*[281].

[281] Mediante STC 341/1993 del 18 de noviembre, se declaró la inconstitucionalidad de esa norma por parte del Tribunal Constitucional Español.

Conforme a la doctrina sentada en la STC 22/1984, de 17 de febrero, y perfilada en la STC 160/1991, de 18 de Julio, comenta Luciano Parejo Alfonso[282] con respecto a la inviolabilidad del domicilio:

a) Tiene por finalidad garantizar el ámbito de privacidad de la persona.

b) Ese ámbito, que es limitado, es precisamente el que ha sido elegido por la propia persona y permite que ésta viva sin sujeción a los usos y convenciones sociales, ejerciendo en él, por tanto, su libertad más íntima.

c) El ámbito en cuestión aparece caracterizado por su exención e inmunidad a las invasiones o agresiones exteriores, tanto de otras personas como del poder público. Y, desde el punto de vista de su protección, consiste desde luego en el espacio físico en que se concrete, pero también en la emanación de la persona y en la esfera privada de ella.

d) La regla de la inviolabilidad del domicilio tiene, así, un contenido amplio e impone una extensa serie de garantías y facultades, entre las que figuran desde luego las de vedar toda clase de invasiones, incluidas las que puedan realizarse sin penetración directa por medio de aparatos mecánicos, electrónicos u otros análogos.

e) La inviolabilidad del domicilio sólo cede en los tres supuestos taxativos contemplados directamente por el texto constitucional: el consentimiento del titular, el flagrante delito y la resolución judicial.

Se debería entender el domicilio como el espacio en el cual un individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales, donde ejerce

[282] PAREJO ALFONSO, L., "El derecho fundamental a la intimidad", IUS ET PRAXIS, Lima, *Revista de la Universidad de Lima,* No. 21-22, 1993, pp. 52-53.

su libertad más íntima, razón por la cual se protege no solo el espacio físico, sino que en este haya un desarrollo de la persona y su esfera privada.

En los casos relacionados con la inviolabilidad del domicilio la regla es la imposibilidad de ingreso, la cual actúa como garantía frente a posibles violaciones. Por el contrario, en caso de permitirse el ingreso o registro, debe resguardarse la proporcionalidad de la medida con las razones que la justifican, medida que debería ser aplicada de forma motivada.

En el artículo 23 de la Constitución costarricense, se establece como garantía la inviolabilidad del domicilio y todo recinto privado de los habitantes de la república. Así mismo, en el contenido del artículo se establecen los límites o excepciones, que consisten en los casos en que éstos recintos pueden ser allanados por orden escrita de un juez competente, o para impedir la comisión o la impunidad de delitos, o evitar daños graves a las personas o a la propiedad, todo ello con sujeción a lo que se establece en la ley.

En SSC 3834-92 de las 19:30 hrs. del 1 de diciembre de 1992[283], con respecto a la inviolabilidad de domicilio, se podría extraer como conclusiones que:

---

[283] Esta sentencia se refiere a la Consulta Facultativa de Constitucionalidad relacionada con un proyecto de Ley de Tránsito, en la cual los diputados consultantes se refieren, en lo que respecta a la inviolabilidad de domicilio, a dos normas en particular. **1.**La primera se refiere a la potestad de las autoridades de tránsito de ingresar a los establecimientos públicos o privados de uso público así como calles privadas a petición de un dueño, a lo que se indica: *"En el primer supuesto -ingreso para fines de mera investigación-, la única forma constitucional que podría estar aplicada sería la del artículo 23, que consagra la inviolabilidad del domicilio y cualquier otro recinto privado de los habitantes de la República; concepto éste del que están excluidos los establecimientos o zonas que, aunque privados, estén destinados a un uso o acceso público o, al menos, colectivo -como sucede por ejemplo con las áreas para comensales en los restaurantes o para clientes en los comercios, o precisamente con las calles internas de una urbanización privada-, los cuales obviamente no tienen el carácter de "recintos privados", por lo que no resulta inconstitucional este aspecto de la ley".* Sigue con relación al primer punto y dice: *"Todo lo anterior debe entenderse siempre dentro de las limitaciones resultantes de que en estos casos se encuentran de por medio derechos y libertades*

a) El domicilio o recintos privados (que no estén dispuestos al público) son inviolables.

b) Los lugares privados de acceso público o uso público y, desde luego, los lugares públicos no tienen el carácter de recintos privados.

c) No todos los supuestos que integran la vida privada de una persona conforman la intimidad, sino solo aquellos que se tipifiquen como pertenecientes al ámbito de reserva de la existencia de cada individuo, tales como cualidades, defectos, enfermedades, estados psíquicos, hábitos, relaciones íntimas, flaquezas, miserias humanas, es decir datos, hechos o, situaciones reservadas al conocimiento de la comunidad, cuya divulgación o conocimiento por otros traiga aparejado algún daño.

---

fundamentales y, por ende, dentro de sus rigurosos límites generales de razonabilidad, proporcionalidad y normalidad, que, además, obligan a interpretar restrictivamente las limitaciones posibles. Así, por ejemplo la investigación de un hecho de tránsito no faculta al inspector para que viole la propiedad estrictamente privada o el domicilio de un ciudadano, pues para ello requiere orden escrita, sólo escrita y nada más escrita de Juez competente, pero sí estaría facultado para ingresar -incluso sin consentimiento- para impedir la comisión o impunidad de delitos o evitar daños graves a las personas o a la propiedad, -en cuyos casos se haría la investigación correspondiente a efecto de determinar si efectivamente se estaba ante esos supuestos y no ante un abuso de poder-. La Sala es consciente de que hay buenas razones para suponer que el proyecto de la Ley en consulta tiene su origen en la necesidad de hacer frente a insuficiencias de la actual Ley de Tránsito, pero ello no justificaría que se desconstitucionalicen derechos, como el de la inviolabilidad del domicilio y de la propiedad". En lo que se refiere a este último aspecto, termina indicando, que el consentimiento permite el ingreso legítimo a las calles de uso común, con el solo consentimiento de uno de los vecinos del lugar. **2.** El otro supuesto, analizado en esa sentencia, relacionado con el domicilio, y, analizado en esa misma sentencia, se refiere a obligación de suministrar la dirección del domicilio –en este caso de un conductor- para efectos de que emita o renueve la licencia para conducir. Y, razona: *"…no todos los supuestos que integran la vida privada de una persona conforman la intimidad, sino solo aquellos que se tipifiquen como pertenecientes al ámbito de reserva de la existencia de cada individuo, tales como cualidades, defectos, enfermedades, estados psíquicos, hábitos, relaciones íntimas, flaquezas, miserias humanas, es decir, datos, hechos, situaciones reservadas al conocimiento de la comunidad, cuya divulgación o conocimiento por otros traiga aparejado algún daño y segundo porque al dar el domicilio no se produce ni daño moral ni patrimonial en perjuicio del informante. Hay que tener presente que para una buena seguridad social, en algunas situaciones se justifica que se limite el derecho a la intimidad de los particulares, pero todo dentro del parámetro de constitucionalidad, y en el caso de estar comunicando cada cambio de domicilio, lo incómodo de la regla no la convierte en inconstitucional".*

De forma general las limitaciones o excepciones legales a la garantía constitucional, tal y como se indicó, están señaladas de forma taxativa en el artículo 23 de la Constitución y se disponen de la siguiente manera: 1) que un juez competente en orden escrita así lo disponga, 2) que se realice para impedir la comisión o impunidad de delitos, 3) o para evitar daños graves a las personas o a la propiedad.

La Sala Constitucional costarricense, ha estimado que el derecho a la inviolabilidad de domicilio se traduce en una tutela de carácter instrumental que defiende los ámbitos en que se desarrolla o puede desarrollarse la vida privada de la persona, de ahí que existe un nexo de unión indisoluble entre la norma que prohíbe la entrada y registro en un domicilio u otro recinto privado y la que impone la defensa y garantía del derecho a la intimidad.[284]

En Costa Rica, el legislador constituyente, a través de las distintas constituciones que han regido al país desde la época de la independencia del Gobierno Español, ha elevado a rango constitucional a la garantía en cuestión.

La Constitución de 1844, en sus artículos 37 y 38, señala el derecho, donde recoge los textos de los artículos 175 y 169 de la Constitución Federal de Centroamérica con las reformas del año 1835 y de 1824.

La Constitución Política de 1847, en sus artículos 19 y 20, consagra, nuevamente, la garantía; el primero repite el texto del artículo 37 de la constitución anterior y el segundo amplía la posibilidad del registro de los documentos privados a los casos de trastorno del orden público, mediante la intervención de autoridad

[284] SSC 3013-94 de las 15:03 del 22 de junio de 1994 y 0627-93 de las 16:03 hrs. del 08 de febrero de 1993.

competente, mientras que la constitución anterior contemplaba la excepción, únicamente, en el caso de traición a la patria.

En lo que respecta a la garantía en la llamada Constitución Reformada de 1848, su regulación se dejó al legislador común al prescribir que los papeles y correspondencia particular no podían ser interceptados ni examinados salvo por la autoridad y en los casos previstos por la ley.

La Constitución de 1859 retoma nuevamente la garantía constitucional dándole una protección plena al disponer el texto del artículo 27 lo siguiente: "*En ningún caso se podrán ocupar, ni menos examinar, los papeles privados de los habitantes de la República."* El artículo 28 del mismo cuerpo de leyes dispuso: *"Es inviolable el secreto de las cartas; las que fueren sustraídas no producen efecto legal."*

La Constitución de 1869, en sus artículos 26 y 27, mantuvo incólume la referida garantía constitucional y en cuanto a la Constitución de 1871, vigente hasta el año de 1948, recogió el mismo texto de las constituciones de 1859 y 1869 y salvo el pequeño lapso con la Constitución de 1917, en la que recibió la garantía en cuestión un tratamiento más restrictivo, permitiendo, únicamente, el registro de cartas y papeles privados con el objeto de llevar prueba a los estrados judiciales, salvo en procesos políticos y remitía a la ley en cuanto a la competencia, casos y formas en los que podrá llevarse a cabo el registro.

Es evidente que al llegar al año de 1948, en cuanto a la evolución del trato constitucional a la inviolabilidad de los documentos privados, emerge un carácter definitivo de protección frente a las intervenciones tanto de los particulares como de la autoridad pública.

En la Asamblea Nacional Constituyente para la Constitución vigente de 1949, este tema fue, ampliamente, discutido con relación al artículo 31 de la Constitución de 1871 y con base en un texto presentado por la fracción social demócrata: *"Son inviolables los documentos privados y las comunicaciones escritas u orales de*

los habitantes de la República. Sin embargo, la ley fijara los casos en que los tribunales de justicia podrán ordenar el secuestro, registro o examen de documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento. Igualmente, la ley fijara los casos en que a los funcionarios competentes les sea permitido revisar los libros de contabilidad y sus anexos, por ser indispensable para fines fiscales o económicos del Estado. En todo caso se guardará secreto acerca del contenido de los documentos ocupados o examinados, hasta donde ello fuere compatible con los fines que motivaron la ocupación o examen".[285]

En esencia se estima que la inviolabilidad del domicilio constituye una garantía acogida en la normativa constitucional y jurisprudencia nacional. Sin embargo, luego se han planteado procesos de amparo relacionados con los recintos privados a los que se refiere la norma constitucional (en el caso del artículo 23 de la Constitución Política) lo que permitió a la Sala Constitucional disponer que el concepto de ese recinto aplica tanto a bienes muebles como inmuebles.[286]

En ese sentido, apunta Fernández Esteban que no puede considerarse domicilio, todo espacio en el que se protege la vida privada. Así, determinado espacio, como los despachos no privados o los coches, pueden estar incluidos en la noción de intimidad, pero no están protegidos por la inviolabilidad del domicilio.[287]

En SSC número 2001-5415 de las 15:11 del 20 de junio de 2001, la Sala Constitucional cambió el criterio inicialmente utilizado y, se indicó, hablando de la

---

[285] Acta No.105, Asamblea Nacional Constituyente, Imprenta Nacional, 1952, Tomo II, Pág. 491.

[286] SSC 627-93. "…*es ineludible que el vehículo sí constituye un recinto privado, pues como en lenguaje común "recinto" significa espacio comprendido dentro de ciertos límites, no cabría distinguir si se trata de bienes muebles o inmuebles". Cfr.* SSC número 08-9690 de las 15:12 hrs. del 30 de julio de 2008.

[287] FERNÁNDEZ ESTEBAN, M. L., *Nuevas tecnologías, Internet y derechos fundamentales,* Mc Graw Hill, Madrid, 1998, p. 125.

garantía de la inviolabilidad del domicilio, que no puede entenderse igual para el caso de los vehículos, pues al ser un medio de transporte que se desplaza en vías públicas y que por ende, ya solo por ese hecho, se ve mucho más limitada la actuación de las personas que tratándose de su residencia, pues si bien se tiene derecho a la intimidad, no se pueden realizar las mismas actividades personales que en el domicilio, precisamente por lo público que puedan resultar dependiendo de dónde se ubique el vehículo, lo cual, eventualmente, podría dañar la moral, el orden público o afectar a terceros, de conformidad con el artículo 28 de la Constitución Política. Por consiguiente, no puede hacerse una equiparación de ambos (domicilio y vehículos), dado que resultan sustancialmente diferentes.

La prueba obtenida a través de la violación del domicilio, de las comunicaciones o de la intimidad, para efectos procesales, resulta inválida tanto en el Derecho Español como en Costa Rica. Para poder obtener esa prueba de forma legal se debe estar en alguno de los supuestos de excepción, los que con claridad se indican en los textos constitucionales y las leyes que regulan las actuaciones de las autoridades públicas.[288]

[288] Tanto la inviolabilidad del domicilio como el secreto de las comunicaciones son garantías que, según el art. 55.1 CE, pueden ser suspendidas en caso de declaración del estado de excepción o de sitio, en los términos previstos por la ley reguladora de dichos estados especiales (LO 4/1981, de 1 de junio). Asimismo, ambos derechos pueden ser suspendidos en los términos previstos mediante ley orgánica, a título individual y con la necesaria intervención judicial y el adecuado control parlamentario, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas (art. 55.2 CE). Dicha previsión constitucional está desarrollada por el legislador en el marco de la Ley de Enjuiciamiento Criminal. LÓPEZ GUERRA, L., *et.ál.*, *op. cit.,* [versión para lector digital Kindle].

4. SECRETO DE LAS COMUNICACIONES.

El secreto de las comunicaciones constituye otra de las garantías esenciales de la vida privada[289], para asegurar la libre injerencia de terceros o los poderes públicos en el ámbito privado de las personas. Se entiende como la libertad de relacionarse con otra u otras personas distantes, a través de un medio destinado al efecto, que trascienda el contenido del proceso comunicativo.

Aunque esta protección tiene sus orígenes en el correo postal[290], hoy día abarca los medios de comunicación orales, escritos y electrónicos, aunque estas últimas no se hayan mencionado de forma expresa en los textos constitucionales.

La doctrina Española, con respecto a las intervenciones de las comunicaciones, es unitaria al estimar que la Constitución menciona de forma expresa las más habituales (en especial, de las postales, telegráficas y telefónicas), pero no ha restringido la garantía del secreto a las formas existentes hoy día, sino que ha formulado la garantía constitucional de una manera genérica (se garantiza el secreto de las comunicaciones), lo que supone comprender tanto las técnicas tradicionales (correo, teléfono, fax), como las de reciente desarrollo (videoteléfono,

---

[289] BELDA PÉREZ-PEDRERO, E., "El derecho al secreto de las comunicaciones", en Parlamento y Constitución, No. 2, 1998, p. 170, [en línea], http://dialnet.unirioja.es/servlet/articulo?codigo=197133

[290] En 1970, la Asamblea Nacional francesa, declaró la inviolabilidad de la correspondencia, con el propósito de eliminar la práctica de los agentes del antiguo régimen de intervenir y leer las cartas de los súbditos. BELDA PÉREZ-PEDRERO, E., *"El derecho al secreto de las comunicaciones", op. cit.*, p. 171. Para Moscoso Segara, el secreto de las comunicaciones es *"concebido como uno de los derechos fundamentales más antiguos, el secreto de las comunicaciones compone una garantía objetiva, protectora de cualquier tipo de comunicación independientemente de su contenido, intúyase por una comunicación de tipo íntimo o alguna otra con carácter trascendente".* MOSCOSO SEGARRA, Alejandro, *"Las intervenciones telefónicas y el derecho a la intimidad"*, Gaceta Judicial, febrero, 2014, [documento electrónico de Vlex].

internet) o las que puedan desarrollarse en el futuro.[291] Este derecho, se concibe como un emanación de la dignidad de las personas, el cual abarca todo aspecto de la vida privada de un individuo con respecto a la protección de injerencias ilegales o arbitrarias[292].

En la constitución española, particularmente en el artículo 18.3, se garantiza la inviolabilidad de las comunicaciones, como una garantía oponible a terceros. Esta garantía se extiende a cualquier comunicación, independientemente del medio utilizado[293].

Este derecho contiene una doble connotación: de forma implícita, la libertad de comunicaciones y, de forma expresa, la garantía de la inviolabilidad. Esta garantía protege la comunicación, frente a terceros, con independencia del contenido que se trate[294], por ello es una garantía objetiva o formal.

---

[291] *Vid.* LÓPEZ GUERRA, L., *et.ál.*, *op. cit.,* [versión para lector digital Kindle]; BELDA PÉREZ-PEDRERO, E., "El derecho al secreto de las comunicaciones", *op. cit.,* p. 170-171; DÍAZ REVORIO, F. J., "El Derecho Fundamental al Secreto de las Comunicaciones: Una Visión Desde la Jurisprudencia Europea y su Influencia en el Tribunal Constitucional Español", en *Revista del Centro Nacional de Derechos Humanos,* pp. 125-126, [en línea], http://www.juridicas.unam.mx/publica/librev/rev/derhumex/cont/2/art/art5.pdf

[292] *Cfr*. CAFFERATA NORES, José I., *Proceso Penal y Derechos Humanos*, Buenos Aires, Editores del Puerto s.r.l., 2000; MARTÍN MORALES, Ricardo, *El régimen constitucional del secreto de las comunicaciones,* Madrid, ed. Civitas S.A., 1995; RODRÍGUEZ RUIZ, Blanca, *El secreto de las comunicaciones (Tecnología e intimidad),* McGraw Hill, Madrid, 1997; MONTERO AROCA, Juan, *La intervención de las comunicaciones telefónicas en el proceso penal: un estudio jurisprudencial*, Valencia, ed. Tirant Lo Blanch, 1999; URBANO CASTRILLO, Eduardo, *El derecho al secreto de las comunicaciones,* Madrid, ed. La Ley 2011.

[293] Al efecto puede consultarse la STC 070/2002, del 3 de abril, en la cual se condenó al recurrente por la prueba obtenida a través de una comunicación escrita, [en línea], http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=14075

[294] El secreto de las comunicaciones abarca la confidencialidad tanto del proceso de comunicación mismo como del contenido de lo comunicado. Se extiende por tanto a aspectos de la comunicación distintos de su contenido, tales como el momento en que tuvo lugar, duración o destino, así como a la identidad de los interlocutores o corresponsales. Todo ello, con independencia del carácter público

Este derecho tiene también una protección supra nacional, pues se reconoce en el artículo 12 de la Declaración Universal de Derechos Humanos[295] de 1948, en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[296] de 1966, en el artículo 8 del Convenio de Roma de 1950, en el art. 7 de la Carta de los Derechos Fundamentales de la Unión Europea y en el art. 11 de la Convención Americana de Derechos Humanos[297] de 1969.

En Costa Rica, el secreto de las comunicaciones se encuentra resguardado en el artículo 24 constitucional, el cual establece:

"Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento. Igualmente, la ley determinará en cuales casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional

---

o privado de la red de transmisión de la comunicación y del medio de transmisión –eléctrico, electromagnético u óptico, etc.- de la misma, ver STC 123/2002, del 20 de mayo, [en línea], http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=14127; *Cfr.* BELDA PÉREZ-PEDRERO, E., "El derecho al secreto de las comunicaciones", *op. cit.*, p. 170.

[295] Art. 12 de la Declaración Universal de Derechos Humanos, 1948, señala: *"Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o su correspondencia, ni de ataques legales a su honra o reputación."*

[296] Art. 17 del Pacto Internacional de Derechos Civiles y Políticos, 1976, señala: *"Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación."*

[297] Art. 11 de la Convención Americana de Derechos Humanos de 1969 señala: *"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."*

y durante cuanto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial. […] *No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación."*[298]

La Sala Constitucional de Costa Rica, en interpretación de la norma citada, diferenció entre documentos privados y comunicaciones escritas y orales, -en estas últimas se incluyen las telefónicas- y señala que se permite el secuestro, registro o examen de los documentos privados excluyendo, expresamente, las comunicaciones, para apuntar además que la correspondencia sustraída de forma indebida no produce efecto legal alguno, y ello es porque las comunicaciones entre los ciudadanos, merecen una protección diferente a la que se le otorga a aquellos otros documentos.[299]

De otra parte, en la jurisprudencia de esta Sala, se ha distinguido entre el rastreo o monitoreo de llamadas y la intervención de comunicaciones. La privacidad de las comunicaciones telefónicas, está protegida en el artículo 24 constitucional y solo puede ser autorizada por un juez en los casos que prevé la ley, mientras que el rastreo de llamadas no está sometido a estas restricciones y no viola el contenido

---

[298] Constitución Política de la República de Costa Rica, Art. 24. *Vid.* CÓRDOBA ORTEGA, J. y GONZÁLEZ PORRAS, A., *Constitución Política de la República de Costa Rica. Concordada y con Jurisprudencia de la Sala Constitucional*, Investigaciones Jurídicas S.A., San José, 2010, pp. 124-125.

[299] SSC número 1261-90 de las 15:30 hrs. del 10 de setiembre de 1990.

del citado artículo constitucional, por lo que lo puede ordenar el Ministerio Público (Ministerio Fiscal) sin autorización jurisdiccional.[300]

En una sentencia reciente, la Sala Constitucional aclaró que el rastreo de llamadas es admisible en casos de ilícitos penales y nunca en el caso de sanciones administrativas y, de mucha importancia, recalcó que *"no puede operar libremente, sino que debe sujetarse también al* ***principio de proporcionalidad.****"*[301] Esta facultad del Ministerio Público –la de ordenar un rastreo telefónico sin orden judicial- opera, como se indicó, solo en el caso de ilícitos penales y, únicamente, contra los sujetos sospechosos y nunca contra un tercero ajeno a la investigación.

Dado que la protección de las comunicaciones no discrimina en cuanto al contenido de estas, no es necesario que, para amparar este derecho, se trate de una comunicación personal, íntima o reservada[302], además, dicha protección se extiende al lugar, la duración e identidad de los interlocutores o corresponsales. Es decir, la protección constitucional se proyecta sobre el proceso de comunicación, con independencia de la técnica empleada.

Con respecto al derecho a las comunicaciones, debe advertirse, que el concepto de comunicaciones debe ser ampliado ante todas las nuevas formas que ofrecen las tecnologías, pues si bien en el concepto tradicional de comunicaciones se protegen las comunicaciones electrónicas, en la práctica se ha visto vulnerado por los registros que quedan en los servidores de las empresas. Sobre los cuales

---

[300] SSC número 2007-17097 de las 9:29 hrs. del 23 de noviembre de 2007 y SSC número 2007-15605 de las 17:35 hrs. del 11 de diciembre de 2007.

[301] SSC número 2014-4035 de las 11:00 hrs. del 21 de marzo de 2014.

[302] El profesor Enrique Belda señala que *"La posibilidad de mantener una comunicación privada ha sido calificada en ocasiones como una faceta del derecho a la intimidad del art. 18.1 CE. Hay que constatar la íntima relación entre el primer y el tercer apartado del art. 18 CE… se comparte una finalidad común de garantía de las relaciones personales, pero el objeto es distinto"*, BELDA PÉREZ-PEDRERO, E., "El derecho al secreto de las comunicaciones", *op. cit.*, p. 170.

se ha interpretado que no requieren de orden puesto que los datos fueron compartidos por los usuarios con la empresa que presta los servicios y el acceso a ese registro no se considera como una intervención de las comunicaciones. Tal interpretación, claramente, resulta contraria a los derechos que se pretenden tutelar por lo cual es necesario que se definan entonces nuevos mecanismos de protección de las comunicaciones.

4.1. Contenido y ámbito de protección.

La titularidad de este derecho es reconocida, al igual que otros derechos de la esfera privada, a las personas físicas y a las jurídicas. El reconocimiento hecho a las personas jurídicas[303], evidentemente, recae sobre las personas físicas que realizan las comunicaciones utilizando los medios de la empresa, que en caso d reclamos recaerá en sus titulares o designados la representación.

La protección de este derecho abarca de forma extensiva, el contenido, el medio o soporte y las circunstancias que la rodean. Así, por ejemplo, podría afirmarse que se debería de proteger: a) la identidad de las personas intervinientes en una comunicación, b) el medio o soporte, lo cual incluye el lugar y rastreo de esa comunicación y, c) el contenido mismo de la comunicación, aunque en esta no se trate de asuntos propios de la intimidad de los intervinientes.

Para que aplique la protección al secreto de las comunicaciones, deben concurrir todos los siguientes requisitos[304]:

a) Utilización de un soporte de comunicación o medio de correspondencia. Debe existir un emisor y un receptor que puedan intercambiar un mensaje. En los medios en los cuales el receptor es pasivo como la prensa, la radio o la televisión, no se podría amparar este derecho.

---

[303] Enrique Belda, señala que *"la protección de las personas jurídicas, en el desarrollo de su actividad, necesitan de la protección de este derecho que tiene una naturaleza personal, pero a la vez reúne los caracteres racionalmente necesarios para su adjudicación a las mismas (igual que, por ejemplo, se les atribuye la titularidad sobre el derecho a la inviolabilidad de domicilio)."*, BELDA PÉREZ-PEDRERO, E., "El derecho al secreto de las comunicaciones", *op. cit.,* p. 173; VERA SANTOS, J. M., "Derechos fundamentales, Internet y nuevas tecnologías de la información y de la comunicación" en GARCÍA MEXÍA, P., "El Derecho de Internet", en GARCÍA MEXÍA, P. (dir.) *Principios de Derecho de Internet*, Tirant lo Blanch, Valencia, 2a ed., 2005, p. 205.

[304] BELDA PÉREZ-PEDRERO, E., "El derecho al secreto de las comunicaciones", *op. cit.,* p. 174-175.

b) Distancia física entre los intervinientes. La transmisión de la comunicación deberá ocurrir a distancia, por lo cual no se protegerían las comunicaciones en presencia física de los participantes.

c) Privacidad de la comunicación. La comunicación debe efectuarse entre dos personas o más, de forma privada y no pública, la comunicación se realiza por lo general de forma secreta y para compartirla deberá haber acuerdo entre los participantes, pues de lo contrario se violaría la intimidad de estos.

Para que exista la protección de las comunicaciones, deberán concurrir los aspectos o requisitos señalados con anterioridad. Evidentemente, existen supuestos en los cuales, el derecho o la protección de las comunicaciones se puede levantar, estos son los casos de excepción y deben estar señalados en la ley.

La Corte Interamericana de Derechos Humanos ha señalado que el derecho a la vida privada se configura como límite a las injerencias abusivas o arbitrarias por parte de los Estados, y que este derecho no es absoluto, sino que su protección está sometida a ciertas limitaciones o excepciones que el mismo ordenamiento jurídico prevé, para casos excepcionales, en aras de garantizar el orden público. Tales excepciones deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática[305].

[305] *Vid.* Corte IDH, Caso Tristán Donoso vs. Panamá, del 27 de enero de 2009, [en línea], http://www.corteidh.or.cr/cf/Jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=253&lang=es

4.2. Excepciones.

Se estima que el derecho al secreto de las comunicaciones se constituyó, en el origen, como una de las manifestaciones del derecho a la intimidad, sin embargo, su actual tutela es autónoma y no depende de este derecho para su protección pues, las comunicaciones son protegidas con independencia del contenido de estas. Ahora bien, como la mayoría de los derechos fundamentales posee límites que permiten, en supuestos de excepción, la intervención, claro está, con el cumplimiento de requisitos que, por lo general, están desarrollados mediante leyes.

En Costa Rica, se desarrolla tal posibilidad en la Ley sobre el registro, secuestro y examen de documentos privados e intervención de las comunicaciones, Ley No. 7425, de 09 de agosto de 1994, la cual permite a los Tribunales de Justicia autorizar el registro, secuestro o el examen de cualquier documento privado, cuando sea absolutamente indispensable para esclarecer asuntos penales sometidos a su conocimiento, así como, autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, por esas mismas razones.

Para los efectos de esta Ley, se consideran 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[306].

En Costa Rica, se permite la posibilidad de intervención de las comunicaciones, a partir del texto constitucional, al señalarse en el mismo artículo que: *"…la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento. Igualmente,* ***la ley determinará en cuales casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo.****"*[307].

El artículo 3 de la Ley sobre el registro, secuestro y examen de documentos privados e intervención de las comunicaciones, permite el secuestro o examen, mediante resolución fundada de juez, de los documentos sobre los que se ejecutará la medida de registro, secuestro o examen. De otra parte, el artículo 9 de esa ley permite la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, sin embargo, la intervención podrá ordenarse, únicamente, en el caso de una lista taxativa de delitos, a saber:

a) secuestro extorsivo

---

[306] Art. 1 de la Ley sobre el registro, secuestro y examen de documentos privados e intervención de las comunicaciones, Ley No. 7425, de 09 de agosto de 1994, [en línea], 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

[307] Art. 24 de la Constitución Política de la República de Costa Rica.

b) corrupción agravada

c) proxenetismo agravado

d) fabricación o producción de pornografía

e) tráfico de personas y tráfico de personas para comercializar sus órganos

f) homicidio calificado

g) genocidio

h) terrorismo y,

i) los delitos previstos en la Ley sobre estupefacientes

Sólo, en los delitos señalados anteriormente se podrá ordenar la intervención de las comunicaciones, para lo cual se debe cumplir además con otros requisitos como los siguientes:

a) Necesidad y proporcionalidad de la medida. Por un lado, sólo podría ordenarse en caso de ser indispensable y necesaria para esclarecer hechos relacionados con una alguna de las conductas delictivas citadas. Con respecto a la proporcionalidad de la medida, debe entenderse como un equilibrio entre el medio empleado y el fin perseguido, sin que el primero resulte excesivo para la consecución del objetivo.

b) Orden escrita y fundamentada emitida por parte de un juez. La orden que autorice la intervención de las comunicaciones, sean orales o escritas, deberá estar debidamente fundamentada y ordenarse de forma escrita. En esta orden deberá indicarse el hecho que se pretende esclarecer, el nombre del dueño o del usuario del medio de comunicación por intervenir o del destinatario y su vínculo con los hechos, el período durante el cual tendrá vigencia la medida y, el nombre de la oficina y de los funcionarios autorizados para realizar la intervención. Si bien la Constitución Política y la Ley que regula las intervenciones no lo indican de forma

expresa, la orden solamente podría ser dictada por parte de un juez de la materia penal, pues si bien se indica que la facultad recae en los Tribunales de Justicia, se indica, también, que se dicta en los casos en los cuales resulto como prueba de alguna de las conductas delictivas antes citadas.

c) Obtención de prueba indispensable. La intervención de las comunicaciones puede ordenarse únicamente en el caso de que resulte indispensable para obtener prueba de la comisión de alguna de las conductas delictivas.

d) Debe ser practicada por un juez. La labor de intervención de las comunicaciones sólo puede realizarla un juez, lo que representan una verdadera dificultad operativa, según lo han expresado los propios operadores. El juez debe, practicar, de forma personal, la diligencia de escucha, salvo en casos de excepción, en los cuales podrá delegarla en miembros del Organismo de Investigación Judicial o del Ministerio Público[308].

e) Por regla general el plazo máximo de intervención no podrá superar los tres meses, salvo en los casos de extrema gravedad o de difícil investigación, en los que el Juez, mediante resolución fundada, puede disponer una prórroga. Excepcionalmente, se podrán ordenar, por igual plazo, hasta dos prórrogas como máximo.

Si en el transcurso de una escucha telefónica autorizada de conformidad con la ley se descubren otros hechos delictivos que no son parte de la lista taxativa, sería posible esclarecerlos a través de una investigación, para la cual, los registros

---

[308] En SSC 95-3195, la Sala Constitucional costarricense, señaló que no es inconstitucional la frase que dice *"podrá delegarla en miembros del Organismo de Investigación Judicial o del Ministerio Público"* [artículo 10 de la Ley], toda vez que lo que puede delegar el juez es, únicamente, la realización de los actos materiales de ejecución de la intervención y no la responsabilidad sobre la misma ni la escucha de las comunicaciones intervenidas.

servirán como noticia del hecho y no como prueba de su ocurrencia o autoría. Es decir, resultan idóneos para que, con base en ellos, se ordene iniciar una investigación, o bien para señalar nuevos rumbos a una que ya se encuentra en curso pero, siempre en el entendido que, carecen de aptitud probatoria para demostrar el hecho -desde que la mera noticia de su ocurrencia no es sinónimo de su demostración- y, en este sentido, constituyen simples hipótesis que habrán de descartarse o corroborarse a través de pruebas idóneas y nunca utilizarse para suplir la ausencia de estas[309].

Debe advertirse, además, que en los casos en los cuales los jueces o intervinientes utilicen la información recabada, mediante el secuestro de documentos o la intervención de comunicaciones, con un propósito distinto al establecido en la orden, podían ser sujetos a la imposición de una sanción penal con prisión de uno a tres años en los casos dolosos y de seis meses a dos años si se trata de casos de negligencia[310].

También, en la normativa penal, se dispuso una sanción para las personas que vulneren las intimidad de otras a través de la intervención de mensajes, datos e imágenes, delito que impone una sanción privativa de libertad de uno a tres años[311].

---

[309] *Vid.* Resolución de la Sala Tercera de la Corte Suprema de Justicia No. 2012-01383, de las 9:22 hrs. del 31 de agosto de 2012.

[310] Arts. 24 y 25 de la Ley sobre el registro, secuestro y examen de documentos privados e intervención de las comunicaciones, Ley No. 7425, de 09 de agosto de 1994.

[311] Art. 196 del Código Penal de Costa Rica, Ley No. 4573 de 15 de noviembre de 1970. *"Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, se apodere, acceda, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino documentación o comunicaciones dirigidas a otra persona"*.

En España, la Ley de Enjuiciamiento Criminal (LECrim), en el artículo 579[312], regula la intervención de las comunicaciones por orden de juez, situación señalada también en el artículo 18.3 de la Constitución[313], permitiendo una salvedad al secreto de las comunicaciones. Esta intervención debe estar contenida en la ley, pues aunque no se indique de forma expresa, pareciera que aplica lo preceptuado en el numeral 53.1 de CE, al señalar que solo por ley puede regularse el ejercicio de los derecho y libertades del capítulo segundo del título I, entre los cuales se encuentra el secreto de las comunicaciones[314].

De esta manera, el derecho al secreto de las comunicaciones es uno de los derechos que pueden ser objeto de suspensión, tanto individual, para los casos de

---

[312] Art. 579 la Ley de Enjuiciamiento Criminal (LECrim), señala: "*1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.*

2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

3. De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.

4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación."

[313] *Vid.* Constitución Política de España, art. 18.3, [en línea], http://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf

[314] *Cfr.* DÍAZ REVORIO, F. J., "El derecho fundamental al secreto de las comunicaciones", en Derecho PUC, *Revista de la Facultad de Derecho*, No. 59, 2007, p. 165.

investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas (art. 55.2 CE), como colectiva, en los estados de excepción y sitio.

Como ya se adelantó en el apartado anterior, a esta garantía le afecta la orden de la autoridad judicial, que permitiría una escucha legal para luego ser aportada como prueba en un proceso judicial. El TEDH ha hecho hincapié en la necesidad de una regulación muy estricta con respecto a estas intervenciones (caso Kruslin, de 24 de abril de 1990)[315].

Cabe mencionar que existe un proyecto de reforma de la LECrim, el cual ya ha sido aprobado por el Congreso de los Diputados (12 de junio de 2015), pero falta el pronunciamiento del Senado. En este proyecto se aprecia un riguroso tratamiento sobre las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 CE, modifica a partir del Título VIII del Libro II de la Ley de Enjuiciamiento Criminal. Por ahora se limitará a mencionar los títulos de los capítulos modificados y que están relacionados con la interceptación de las comunicaciones.

Según lo anterior, el capítulo I del proyecto mencionado trata sobre la entrada y registro en lugar cerrado y del registro de libros y papeles. El capítulo II se dedica a la detención y apertura de la correspondencia escrita y telegráfica. El capítulo III se refiere a la interceptación de las comunicaciones telefónicas y telemáticas, este procedimiento regula de forma precisa en tres secciones muy detalladas. El capítulo

---

[315] El Tribunal Europeo de Derechos Humanos (TEDH), ha influido, a través de su jurisprudencia, en las leyes de los estados. Señala el Profesor Díaz Revorio, que, en el caso español, la obsolescencia de la Ley de Enjuiciamiento Criminal, y la insuficiente adaptación de esta a los requisitos establecidos en la jurisprudencia del TEDH, ha implicado varias condenas al Estado español por parte del Tribunal de Estrasburgo, así como la necesidad de que fueran el Tribunal Constitucional y Tribunal Supremo, a través de una jurisprudencia exigente que ha incorporado sin reparos los requisitos establecidos en la jurisprudencia del TEDH. DÍAZ REVORIO, Francisco Javier, "El Derecho Fundamental al Secreto de las Comunicaciones: Una Visión Desde la Jurisprudencia Europea y su Influencia en el Tribunal Constitucional Español", *op. cit.,* p. 126.

IV se dedica a la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos. De otra parte, en el capítulo V, se refiere a la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen. Por último, el capítulo VI se refiere al registro de almacenamiento masivo de información[316].

Será necesario un examen riguroso de esta reforma, sin embargo, por ahora se limitó a enunciar los títulos relacionados, para luego en otro apartado hacer alguna referencia particular a algunos de estos, particularmente, al capítulo relacionado con el registro de almacenamientos masivos de información[317].

[316] El texto del proyecto de reforma de la LECrim, puede ser consultado en: http://www.ub.edu/dpenal/recursos/doc_legislacio/LECr_anteproyecto_y_otras_2014.pdf

[317] Vid. *Infra* Capítulo VI.

5. ORIGEN DE LA PROTECCIÓN DE DATOS PERSONALES.

El derecho a la autodeterminación sobre los propios datos personales, consiste en la prerrogativa de la persona para disponer de la información que sobre sí misma exista en los registros o bases de datos, a fin de que esa información sea veraz, íntegra, actualizada, no intrusiva, y con las garantías de seguridad y de uso conforme a la finalidad para la que fue proporcionada.[318]

Uno de los primeros precedentes de la protección de la privacidad y sobre el control de los bancos de datos, públicos y privados, fue la ley dictada por el Parlamento sueco el 11 de mayo de 1973, reformada en 1979 con algunas variaciones de texto, la cual contenía veinticinco artículos y varias disposiciones transitorias[319].

Sin embargo, para Téllez Aguilera[320], la primera ley de protección de datos que como tal aparece en Europa fue la formulada en el Land de Hesse (uno de los 16 Estados federados de Alemania) el 7 de octubre de 1970, con 17 artículos, relacionados a la protección de datos informáticos o aquellos susceptibles de serlo por parte de la administración pública del Estado. Posteriormente, se aprobó la Ley 289 de Protección de Datos Sueca de 11 de mayo de 1973, la cual prohibía crear registros sobre antecedentes judiciales y sobre los denominados “datos sensibles”,

---

[318] AVELEYRA, A. M., *El derecho de acceso a la información pública vs. El derecho de libertad informática* [en línea], http://profesor.sis.uia.mx/aveleyra/comunica/pdp.htm

[319] FRONSINI, V., “Bancos de Datos y Tutela de la Persona”, *op. cit.*, p. 29 y ss.

[320] TÉLLEZ AGUILERA, A., *La Protección de Datos Personales en la Unión Europea. Divergencias normativas y anhelos unificadores,* Editorial Edisofer S.L., Madrid 2002, p. 28.

cuyos ficheros podían ser creados únicamente por la administración pública, salvo casos expresamente autorizados.

El 26 de septiembre de 1973, el Comité de los Ministros del Consejo de Europa adoptó la resolución número 22 sobre la “protección de la vida privada de las personas físicas respecto a los bancos electrónicos de datos en el sector privado”, y sólo un año después, el 20 de septiembre de 1974, adoptó la resolución número 29 que estableció pautas ordenadoras de los bancos de datos del sector público y, aunque se trataba de recomendaciones, constituyeron un gran aporte y ejercieron importante influencia en Europa.

También en 1974, se aprobó en EE.UU. el *Privacy Act,* el 31 de diciembre de 1974, de gran importancia por la producción de computadoras en ese país. Posteriormente, como respuesta del Derecho a la protección de datos, en 1985 se aprobó la *Electronic Communications Privacy Act* de 1985 y, posteriormente se aprueban la *Patriot Act* de 2001 y la *Can-Spam Act* de 2003.

La protección de datos se configura como un derecho fundamental de la persona, que se concreta en el amparo, debido a la posible utilización de terceros en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado.

En la Constitución de Portugal de 1977 se introduce en el artículo 35 el principio de que cada ciudadano tiene el derecho de conocer sus datos personales recopilados en los bancos de datos y su utilización, así como el derecho de pretender su corrección y su actualización.

En 1978 se establece, en el artículo 18 de la Constitución Española que una ley especial limitará la utilización de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el completo ejercicio de sus derechos, lo cual se dio hasta 1992 con la LORTAD.

A partir de 1975 varios Parlamentos de los Estados europeos aprueban nuevas formas de garantía jurídica para la protección de datos. A estas iniciativas legislativas pueden agregarse también la de dos países pertenecientes a la *Commonwealth* británica: Nueva Zelanda, que en 1976 aprobó el *Wanganui Computer Centre Act*, y Canadá, donde el 2 de junio de 1977 entró en vigor el *Human Rights Act*, los cuales brindaron protección jurídica a los datos personales.

En 1978 en Europa se aprueban las siguientes leyes: el 6 de enero, en Francia, la ley relativa a la informática, a los archivos y a la libertad; el 8 de junio, en Dinamarca, la ley sobre los registros privados, seguida por la de los registros públicos; el 9 de junio, en Noruega, la ley sobre los registros de datos personales, vigente desde el 1 de enero de 1980; el 18 de octubre, en Austria, la ley sobre la protección de los datos personales, precedida y preparada por un proyecto de ley gubernativo presentado en el Parlamento en diciembre de 1975; el 31 de marzo de 1979, el Gran Ducado de Luxemburgo también emanó la ley para reglamentar la utilización de los datos nominativos en los procesamientos informáticos; y en 1976, en Bélgica y en Holanda se prepararon proyectos orgánicos que, después de varias modificaciones ya han sido convertidos en leyes formales.

De esta manera, la Comunidad Europea, a través de sus órganos, dictaron una serie de Directivas, tendientes a proteger los datos personales, la que se exponen a continuación:

La Directiva 1995/46/CE el 24 de octubre de 1995 (relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos) puede ser considerada, a la fecha, la norma principal sobre la protección de datos personales.

La Directiva 97/66/CE[321], del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

La Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

La Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, 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.

La Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de

[321] En el art. 1 se señala que “la armonización de las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las telecomunicaciones, así como la libre circulación de tales datos y de los equipos y servicios de telecomunicación en la Comunidad”.

las comunicaciones electrónicas y el Reglamento (CE) 2006/2004 sobre la cooperación en materia de protección de los consumidores.

La Directiva 2009/140/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 mediante la cual se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

De otra parte, el Tribunal Constitucional Federal Alemán, mediante sentencia del 15 de setiembre de 1983 confirmó el derecho a la autodeterminación informativa[322], completando el catálogo de los llamados derechos constitucionales de la personalidad, pese a la inexistencia de un derecho específico como el erigido en la Ley Fundamental de 1949.

Este Tribunal resolvió el recurso presentado contra una Ley del 25 de marzo de 1982 relativa al Censo Demográfico *et al Volkszählungsurteil* [323]; la declaró inconstitucional, en razón del excesivo número de datos o informaciones solicitadas a los ciudadanos (recolección indiscriminada de datos), con el fin de ser sometidos a un posterior tratamiento informatizado. El agravio consistía en el riesgo de la posible combinación de datos y su adscripción a una determinada persona. El

---

[322] La esencia del derecho de autodeterminación informativa -*Recht auf informationelle selbsbestimmum*-, se resume en la sentencia como la posibilidad del individuo de determinar quién, qué y con qué finalidad puede conocer o utilizar un tercero esos datos. De esta forma, intimidad no es solo el aislamiento o la reserva del individuo, sino también el control de lo externo a nosotros y que le pertenece o, al menos, le pertenece a su vida privada.

[323] Ver en ese sentido HASSEMER, W. y CHIRINO SÁNCHEZ, A., *El Derecho a la Autodeterminación Informativa y los Retos del Procesamiento Automatizado de Datos Personales,* Editorial del Puerto s.r.l, Buenos Aires, 1997, pp. 5-6. *Cfr.* DARANAS PELAEZ, Manuel (trad.), "Jurisprudencia constitucional extranjera. Tribunal Constitucional Alemán". Ley del Censo, BJC, número 33, 1984.

Tribunal señaló como principio básico del ordenamiento jurídico el valor y la dignidad de la persona que actúa con libre autodeterminación al formar parte de una sociedad libre. Agregó que no sería compatible con el derecho a la autodeterminación informativa, un orden social y jurídico que hiciese posible que un ciudadano *"no pueda percibir con suficiente seguridad qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decir por autodeterminación informativa. (…). Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos"*.[324]

En otras palabras, la persona posee la autodeterminación informativa como una facultad para el resguardo del derecho a la intimidad, haciendo especial hincapié en la necesidad de evitar la elaboración de un perfil de la persona a partir de la interacción de archivos que guardan distintos datos personales del individuo. El Tribunal Alemán configuró el derecho a la autodeterminación a partir del derecho general de la personalidad garantizado en la Ley Fundamental de Bonn y la facultad del individuo a tener potestad e injerencia en el manejo que las entidades públicas y privadas hagan sobre sus datos personales.

El Tribunal Federal Alemán de forma determinante señaló que la persona posee un derecho de libre decisión y libre disposición sobre sus datos personales, lo cual le faculta para decidir qué es lo que otros pueden saber sobre él. Si bien

[324] Sentencia de 15 de diciembre de 1983 del Tribunal Constitucional Alemán ref. 1 BvR 209/83.

confirmó la validez de la mayor parte de la ley, obligó a realizar modificaciones en ciertos puntos, en su mayoría, relativos al modo en que se podía autorizar la recolección y almacenamiento de los datos, lo cual significó, finalmente, que el censo se postergara por cuatro años con un considerable costo para el Estado, pero con un papable beneficio para los particulares[325].

Como se desprende de lo anterior, el derecho a la autodeterminación informativa tiene un contenido diferente al derecho a la intimidad, su ámbito es más amplio y los elementos que los componen resultan más complejos. Hay quienes consideran que este derecho debe protegerse de forma independiente con respecto al derecho de intimidad, de ahí que se configure como un derecho fundamental autónomo. Para algunos, este derecho constituye el derecho fundamental característico de esta faceta del mundo social que comúnmente llamamos Sociedad de la Información.

De esta manera, Hassemer y Chirino afirman que *"Un progreso de las tecnologías de la comunicación e información que no tenga una vinculación con los derechos fundamentales no sería ninguna modernización sino un retroceso"*.[326]

Apuntan que el desarrollo hacia un derecho a la protección de datos no fue una invención, sino más bien un avance hacia el entendimiento de los derechos del hombre y el ciudadano como una herramienta en contra de una amenazante actuación del Estado.[327]

Existen posiciones que plantean la reflexión sobre la libertad de información puesto que, este derecho admite limitaciones frente al derecho a la intimidad. Se

---

[325] KOMMERS, D., "The Constitutional Jurisprudence of the Federal Republic of Germany", Durham, Londres, 1989, p. 332.

[326] HASSEMER, W., y CHIRINO, A., *op. cit.,* p. 13.

[327] *Ibíd.,* p. 30.

presentan como derechos en permanente conflicto, lo cual implica la posibilidad de proteger, el derecho a la intimidad, en forma preventiva. Lo anterior se fundamenta en el hecho que, el derecho a la información y a la vida privada, son derechos fundamentales de igual rango o consagración constitucional, cuya vigencia es necesaria para una sociedad democrática, derechos que no pueden ser protegidos de forma adecuada si las vulneraciones o agresiones no son previstas con anterioridad, máxime si cuando se vulnera la intimidad no es necesaria la eximente de verdad o *exceptio veritatis* como ocurre con la vulneración del derecho al honor. Lo anterior, siempre y cuando, no se presenten razones justificantes de interés general o público que manifiesten la necesidad de divulgación de aspectos personales o familiares de una persona.

El Tribunal Constitucional Español[328], en la sentencia 292/2000 de 30 de Noviembre de 2000, ha reconocido la existencia de un nuevo derecho fundamental: el derecho a la protección de datos, que es distinto del derecho a la intimidad. Este derecho lo define como el poder de control de la persona sobre sus datos personales, sobre su uso y destino. Es un poder de disposición permanente sobre todos los datos relacionados con la persona, que deben ser protegidos en su ejercicio, de forma que cualquier persona tenga capacidad de control sobre los mismos y conozca, en todo momento, quiénes tienen sus datos, con qué finalidades y pueda negarse a facilitarlos o bien modificarlos, pues de lo contrario, este nuevo derecho quedaría vacío de contenido. El derecho a la intimidad personal y familiar y el derecho a la protección de datos, aun siendo distintos tienen una base común: la dignidad de la persona humana y los derechos inviolables que le son inherentes.

[328] Esta sentencia es de suma importancia con respecto a la valoración de la autodeterminación informativa, pues reconoce de forma expresa este derecho fundamental como autónomo y con un contenido diferente del derecho de intimidad. El Tribunal reconoce que el artículo 18 inciso 1 de la CE no brinda una protección suficiente frente a la nueva realidad derivada de los avances tecnológicos, por esta razón, el constituyente garantizó en el inciso 4 de esa norma la protección idónea y específica para la protección de los datos personales.

La Sala Constitucional de Costa Rica ha considerado este derecho en sentencia número 1999-004847 de las dieciséis horas con veintisiete minutos del veintidós de junio de mil novecientos noventa y nueve de la siguiente manera:

"(…) tanto en el plano internacional como en el interno, el Derecho vigente en Costa Rica protege el derecho a la intimidad como protección del individuo en relación con su vida privada. No obstante lo anterior, la capacidad de archivo y de transmisión de los datos almacenados por parte de las grandes corporaciones públicas y privadas, ha hecho posible que la vida de los ciudadanos pueda con facilidad estar al alcance de una gran cantidad de personas, por lo que su tutela real se tornaría insuficiente si se limitara únicamente a la esfera de protección enmarcada dentro del derecho a la intimidad. En razón de ello y a efectos de no hacer nugatorio lo dispuesto en el artículo 24 y en el sistema constitucional costarricense como un todo, su ámbito de cobertura ha evolucionado relativamente al desarrollo de los medios de información y comunicación, cuyo nivel de complejidad ha permitido el archivo de cantidades de datos cada vez más grandes sobre las personas y ha abierto la posibilidad de procesar esa información con un alto grado de precisión y en muy poco tiempo, por lo que, con este avance sus ataques no solo se tornan más frecuentes, sino también más graves. Las informaciones reservadas y clasificadas en bases de datos o en cualquier otra forma de almacenamiento de información pueden ser utilizados con distintos fines y en ellos entra en conflicto el interés del Estado o entes particulares de contar con información para el cumplimiento de sus fines, con el del sujeto sobre quien versa la información recabada y que cuenta a su favor con un derecho a su intimidad, que se dirige a que éste pueda desarrollarse con plenitud y sin interferencias en su esfera personal. Con base en lo expuesto, considera este Tribunal que, dado el gran avance tecnológico, la inmersión de los medios informáticos en la esfera del individuo no es susceptible únicamente de lesionar su intimidad, pues muchos de los datos contenidos en esos archivos son públicos, y aun así el uso indiscriminado de tales informaciones puede ocasionar graves perjuicios al ciudadano, si aquel no se sujeta a ciertos parámetros de veracidad y razonabilidad. La protección estatal, por ende, no debe estar sólo dirigida a tutelar la intimidad del individuo, sino que debe ir más allá: debe controlar el uso que de los datos de las personas -íntimos o no- se haga. Es así como se puede hablar de un verdadero derecho a la

autodeterminación informativa, como principio constitucional desprendible a partir del texto del artículo 24 ya citado."[329]

Tal y como se desprende con claridad de la sentencia citada, el Tribunal Constitucional costarricense reconoce el derecho a la autodeterminación informativa como un principio derivado del artículo 24 de la Constitución Política, sin embargo, al mismo tiempo se le califica como un verdadero derecho, es decir, debe entenderse como un derecho autónomo.

Esta última calificación podría significar que el derecho a la autodeterminación es un derecho autónomo, sin embargo, se constriñe y lo hace dependiente del derecho a la intimidad. Esta diferenciación no tiene ninguna relevancia en la práctica jurídica, pues el derecho a la protección de datos es tutelado por el Tribunal Constitucional (ya sea este derecho derivado o autónomo), sin embargo, se puede considerar que la novedad de esta sentencia es que reconoció la existencia de un nuevo derecho, un derecho producto del surgimiento de nuevas tecnologías de la información y comunicación que amenazaban un derecho ya consolidado como lo era el derecho a la intimidad.

Una diferenciación clara y explicativa, entre intimidad y Autodeterminación Informativa, va a encontrarse en la consagración de ambos derechos en la Carta de los Derechos Fundamentales de la Unión Europea bajo la denominación de "…respeto de la vida privada y familiar" en su artículo 7. Esa norma hace alusión a

[329] SSC número 1999-04847 de las 16:27 hrs. del 22 de junio de 1999. El resaltado se adiciona.

la intimidad de manera concreta y, por otro lado, habla de manera independiente de la "…protección de datos de carácter personal" en el artículo 8.[330]

En ese sentido, Ignacio Subiza apunta que *"el viejo derecho a la intimidad no es suficiente para proteger nuestros derechos fundamentales en el mundo de la informática y de las bases de datos".* [331]

El constante número de casos generados por las innovaciones tecnológicas que afectan de forma grosera el derecho de intimidad, ha justificado una preocupación creciente entre los usuarios de estas tecnologías, haciendo que cada vez más se preocupen por los datos que generan.

Basta con hacer una pequeña búsqueda en Internet con las palabras privacidad o intimidad para que aparezcan una gran cantidad de casos relacionados con nuevas actividades de las empresas que se encuentran al margen de la regulación constitucional.

Una reciente creación legislativa, relacionada con la protección de datos, en Costa Rica, dispone en el artículo 8 inciso c) (Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, Ley número 8968 del 7 de julio del 2011), que el derecho a la autodeterminación informativa se encuentra limitado en los casos de prevención, persecución, investigación, detención y represión de las infracciones penales, límites que ya han sido tratados en la jurisprudencia nacional.

---

[330] *Carta de los Derechos Fundamentales de la Unión Europea*. Art. 7 "…respeto de la vida privada y familiar" esa norma hace alusión a la intimidad de manera concreta y, por otro lado, el art. 8 indica, de manera independiente, sobre la "…protección de datos de carácter personal".

[331] SUBIZA PÉREZ, I., *La protección de datos y sus mundos. La construcción del derecho a la protección de datos personales como un derecho autónomo,* DAPP Publicaciones Jurídicas, Madrid, 2009, p. 26.

En relación a los límites y algunos otros supuestos relacionados con este tema, se exponen a continuación varios casos jurisprudenciales para que se tenga una idea de cómo se perfila la tutela constitucional.

Con respecto a llamadas telefónicas mortificantes para el cobro de deudas crediticias, la Sala Constitucional ha emitido un nuevo criterio, a raíz de un Decreto Ejecutivo que regula el procedimiento administrativo para la atención de denuncias por este tipo de hechos. En estos supuestos ahora el Tribunal remite a la jurisdicción ordinaria mientras que, con anterioridad, solía resolver por el fondo los casos denunciados.[332]

Sobre los procedimientos administrativos en los que se han utilizado como modos de investigación los seguimientos de personas y vigilancias estacionarias, la Sala Constitucional ha señalado que estos resultan lesivos, pues se constituyen como intromisiones indebidas a la esfera de la intimidad lo que se traduce en una violación de derechos fundamentales.[333]

En el caso de acceso a registros sanitarios de personas fallecidas, la Sala Constitucional ha estimado que el acceso debe ser garantizado a quienes tienen legitimación para ello. Si bien el acceso a registros médicos le pertenece, en vida, únicamente, al interesado, dicha situación cambia con el fallecimiento de la persona y quedan autorizados para acceder éstos registros quienes tengan legitimación para ello, como ejercicio de los derechos *post mortem* de los familiares supérstites.[334]

---

[332] SSC número 2012-6628 de las 11:42 hrs. del 22 de junio de 2012.

[333] SSC número 2012-13097 de las 11:00 hrs. del 18 de setiembre de 2012.

[334] SSC número 2012-7118 de las 9:30 hrs. del 29 de junio de 2012.

La confidencialidad de los datos personales opera como límite al derecho de acceso a la información según lo dispuesto en el numeral 30 de la Constitución de Costa Rica.

Otro de los límites desarrollado por la Sala Constitucional se refiere a la identidad de las partes que participan en procesos judiciales, y, especialmente, los que tratan asuntos relacionados con la familia o menores de edad. Adicionalmente, se plantea la publicación de estas resoluciones en Internet como una violación al derecho de intimidad de las partes procesales. En ese sentido, estimó la Sala *"…que si bien, las sentencias como tales son documentos públicos y, por ende, su acceso es irrestricto, lo cierto es que, atendiendo a lo dicho, resulta razonable la protección de los datos contenidos en ellas que permitan identificar a las partes involucradas y vincularlas con el conflicto específico. Es claro que la difusión de las sentencias, en este caso, vía Internet, constituye un instrumento necesario para garantizar la transparencia de la Administración de Justicia amén de que es un medio idóneo para que la población tenga conocimiento de los criterios jurídicos que resultan aplicables en las distintas ramas del derecho…"*[335]

En la Ley de protección de la persona frente al tratamiento de sus datos personales se distinguen entonces cuatro categorías de datos personales, con el fin de determinar el grado de protección y acceso a esa información, esto son: los datos sensibles (máxima protección), los datos de acceso restringido (de protección media), lo datos de acceso irrestricto (sin protección) y los datos referentes al comportamiento crediticio (los cuales se rigen por las normas que regulan el Sistema Financiero Nacional).

El derecho a la autodeterminación informativa se configura como una facultad para el resguardo del derecho a la intimidad, haciendo especial hincapié en la

[335] SSC número 2012-3712 de las 9:05 hrs. del 16 de marzo de 2012.

necesidad de evitar la elaboración de un perfil de la persona a partir de la interacción de archivos que guardan distintos datos personales del individuo.

En el *derecho constitucional* moderno se acepta, casi de forma unánime, el derecho de Intimidad y Privacidad, como un derecho fundamental indispensable para que las personas puedan desarrollarse, sin obstáculos ni interferencias en una vida plena y digna.

Este se configura como un derecho subjetivo, positivo y esencial en la organización social. Se trata de una verdadera garantía institucional de pluralismo y democracia. Como premisa se plantea que, si lo público está regido por la pretensión de igualdad y lo privado determinado por la singularidad, podría estimarse que el respeto de esa diferencia, entendida como el respeto a la vida privada, constituye una expresión o manifestación de libertad, como consecuencia directa de la dignidad humana en su condición de fundamento de orden político y de paz social.

El Derecho a la Intimidad se destaca entra los derechos fundamentales a la personalidad y ha sido reconocido desde el siglo XIX, con anterioridad a los derechos sociales, por lo cual se podría ubicar en la primera generación de los derechos humanos. A partir de este derecho se construyeron diversos mecanismos de protección, sirviendo como base de la protección de los datos personales.

Con respecto al contenido esencial de este derecho, no existe un concepto uniforme, sin embargo, la doctrina es mayoritaria al entenderlo como un derecho de la personalidad, el cual se adquiere por la consideración de la condición humana, es decir, estos derechos nacen con la persona y se convierten por ley en un valor jurídico tutelado.

Los orígenes de este derecho se remontan al derecho anglosajón, aunque, muchos autores estiman que, como valor, el concepto se asocia a dos vertientes previas, el cristianismo y su modalidad reformista a finales de la edad media ligada a la desaparición de la sociedad feudal y, de otra parte, con la Revolución Francesa y el eventual surgimiento de la burguesía capitalista, quienes tenían la posibilidad económica y social de apartarse de la sociedad.

El desarrollo doctrinal, normativo y jurisprudencial, así como la tutela de este derecho, demuestra la necesidad de protección de las interferencias de terceros en la vida privada de las personas. Se considera que una de las razones que han ampliado el contenido de este derecho, así como, el reconocimiento de otros derechos que tomaron como punto de partida el derecho de intimidad, está relacionado con la transición a una sociedad tecnológicamente evolucionada.

Es por ello que, en la actualidad, el estudio del derecho a la intimidad cobra relevancia frente a los avances tecnológicos, que en apariencia hace a los individuos más vulnerables a las intromisiones en su vida privada, consecuentemente, en su intimidad.

En una sociedad democrática y respetuosa de los derechos fundamentales, debería ser inaceptable la intromisión arbitraria de particulares o el propio Estado, en asuntos privados de las personas.

En sus orígenes, este derecho se definía como el derecho a ser dejado a solas o a la no intromisión en los asuntos personales o familiares de un individuo sin su autorización; en la actualidad, se concibe como el derecho del individuo a decidir si desea compartir sus pensamientos, sentimientos y los hechos de su vida personal o familiar. Es decir, se trata de un derecho que en un principio tenía una condición prohibitiva a no ser molestado y luego se convierte en un derecho activo, en el cuál el individuo fija sus propios límites a la información que desea hacer del conocimiento de las demás personas.

El desarrollo de la protección de ese derecho se refleja también en los instrumentos del derecho internacional, como producto quizá del avance tecnológico que se ha producido.

El concepto de dignidad se estima como parte de la condición humana y como fundamento de los derechos de la persona, independientemente, de su reconocimiento jurídico, situación que se entiende desarrollada al margen de los derechos reconocidos a las personas. Esta protección supone un gran avance en el

reconocimiento y desarrollo de los derechos fundamentales y libertades reconocidas en las normas constitucionales, que además se deben interpretar en el marco de los derechos protegidos en los convenios y tratados de derechos humanos.

Tomando como punto de partida el derecho de intimidad, se han reconocido otros derechos fundamentales, ahora de forma autónoma, como el derecho al honor, el derecho de imagen, la privacidad del domicilio y las comunicaciones, así como el derecho a la protección de los datos personales.

Estos derechos, como la mayoría de los derechos subjetivos, no son irrestrictos o absolutos, pues contienen límites a su ejercicio. La limitación de estos derechos no es una tarea sencilla, pues esas limitaciones podrían convertir en nugatorio un derecho fundamental ya reconocido.

El constante número de casos generados por la afectación causada por las innovaciones tecnológicas, las cuales vulneran de forma grosera el derecho de intimidad, ha justificado una preocupación creciente entre los usuarios de estas tecnologías, haciendo que cada vez más se preocupen por los datos que generan.

Este desarrollo tecnológico también ha generado la necesidad de reconocer, como derecho independiente y autónomo del derecho de privacidad, al derecho a la protección de datos de las personas, y paralelamente también ha facilitado el surgimiento de mecanismos especializados en su protección, tanto desde la esfera administrativa como en la vía jurisdiccional, desarrollándose una base jurisprudencial que ha enriquecido y consolidado a la protección de datos de las personas como un derecho fundamental.

TERCERA PARTE. DERECHOS RELACIONADOS CON LAS TECNOLOGÍAS INFORMACIÓN Y COMUNICACIÓN.

CAPÍTULO IV. SITUACIÓN JURÍDICA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.

"Privacy is rarely lost in one fell swoop. It is usually eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone."[336]

[336] La privacidad rara vez se pierde de un solo golpe. Por lo general, se erosiona con el tiempo, se disuelve en pequeños trozos casi imperceptible hasta que finalmente se comienza a notar lo mucho que se ha ido, [traducción libre del autor]. SOLOVE, D. J., "Why privacy matters even if you have 'nothing to hide'", en *The chronicle of higher education*, 15 de mayo, 2011, [en línea], http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

1. CONSIDERACIONES PRELIMINARES.

De todos los avances de medios tecnológicos y comunicaciones se podría decir que Internet es uno de los más importantes, sin embargo, no es el único, las redes inalámbricas y terminales móviles ahora interconectados a redes de telefonía e Internet juegan un papel importante en la sociedad. Las comunicaciones tienen una nueva dimensión, un espacio que no conoce fronteras ni controles con la participación de múltiples intervinientes y desde el punto de vista jurídica ha generado gran cantidad de discusiones, conflictos y regulaciones.

De forma muy simple podría definirse Internet[337] como una red que conecta múltiples redes, de distintos tamaños, por lo que se le ha llamado la red de redes. Internet carece de una entidad física y control, está distribuida de forma global y permite la conexión de varias formas o tipos de redes[338]. En términos de regulación jurídica es todo un reto pues tampoco se circunscribe a un país o unión de países, pues como se indicó tiene alcance global. Por supuesto existe variedad de regulaciones y ordenanzas respecto a Internet, siendo la gran mayoría de alcance local.

La red global ha generado muchas posibilidades y trabajos, así como nuevos modelos de negocios, empleos, profesiones, empresas, entro otros. En los aspectos jurídicos, ha sido el detonante de nuevos instrumentos, instituciones, normativa y

---

[337] Se puede entender como la *"Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación"*, Diccionario de la Real Academia de la Lengua Española [en línea], http://lema.rae.es/drae/?val=internet

[338] Internet funciona porque los estándares abiertos permiten que todas las redes se conecten a todas las redes. Esto es lo que hace posible que cualquiera pueda crear contenido, ofrecer servicios y vender productos sin necesitar el permiso de una autoridad central., Internet Society, [en línea], http://www.internetsociety.org/es/c%C3%B3mo-funciona

jurisprudencia, provocando replantear y ajustar la normativa, la que se ha estado adaptando a los usos electrónicos de la sociedad.

La creación de Internet se encuentra documentada desde el año de 1962, por lo que en los próximos apartados se limitará a resumir, solamente, algunos de los aspectos más importantes sobre la creación y su implementación, basta con seguir algunos de los vínculos dejados en el documento para acceder a las diversas fuentes consultadas para profundizar en ese tema. El propósito de este Capítulo es hacer una breve referencia al origen y al desarrollo de la red para sustentar algunos de los objetivos de la investigación planteada.

El uso extensivo de Internet está cambiando a la sociedad, con respecto a las formas de comunicación, comercio, información, educación, entretenimiento, impactando en diversos aspectos de la vida del ser humano[339].

Tanto ha sido el cambio, que ahora hablamos del *Ciberespacio*[340] para hacer referencia a lo inmaterial de Internet, en contraposición de lo territorial o físico. Se refiere a un nuevo ambiente humano y tecnológico que comprende computadoras, redes, sistemas informáticos y personas de todos los países, culturas e idiomas y de todas las edades y ocupaciones, que proporcionan y demandan información.

---

[339] Internet ha revolucionado la informática y las comunicaciones como ninguna otra cosa. La invención del telégrafo, el teléfono, la radio y el ordenador sentó las bases para esta integración de funcionalidades sin precedentes. Internet es a la vez una herramienta de emisión mundial, un mecanismo para diseminar información y un medio para la colaboración y la interacción entre personas y sus ordenadores, sin tener en cuenta su ubicación geográfica. Internet representa uno de los ejemplos más exitosos de los beneficios de una inversión y un compromiso continuos en el campo de la investigación y el desarrollo de la infraestructura de la información., LEINER, B. y otros, "Breve historia de Internet", *Internet Society*, [en línea], http://www.internetsociety.org/es/breve-historia-de-internet#f1

[340] El DLE define Ciberespacio como "el Ámbito artificial creado por medios informáticos"., Diccionario de la Real Academia de la Lengua Española [en línea], http://lema.rae.es/drae/?val=ciberespacio

2. CONCEPTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN Y CARACTERÍSTICAS PRINCIPALES.

Atendiendo a la naturaleza jurídica de este trabajo, un concepto general de tecnologías de la información y comunicación (TCI)[341] es el que probablemente mejor se ajuste a los efectos expositivos, y este se refiere al conjunto de tecnologías y servicios de comunicación e información, que debería incluir tanto las tecnologías de la comunicación, como la informática y los servicios relacionados.

Resulta importante aclarar, desde este punto, que dependiendo del área de aproximación y la disciplina de estudio desde el cual se aborde este concepto, podría variar su contenido, el cual podría ser de una forma genérica o una más técnica, limitando o especificando su estructura y composición. Así mismo, en la mayoría de artículos jurídicos se utilizan otros términos como sinónimos de este concepto, entre otros *"nuevas tecnologías de información y comunicación", o "nuevas tecnologías"* o por separado el concepto de *"tecnologías de comunicación"* y el de *"tecnologías de información".*

El concepto de "tecnologías de comunicación" se refiere al conjunto de instrumentos desarrollados para la comunicación y la transmisión de la información. De otra parte, "*tecnologías de información"* es utilizado para hacer referencia a la

[341] Una aclaración sobre la ausencia de las mayúsculas. El profesor Javier Díaz Revorio planteó una consulta al Departamento de "Español al día" de la Real Academia Española, en la que se indica: la mayúscula no está justificada en el uso genérico de la denominación "tecnologías de la información y la comunicación". Deberá escribirse en mayúsculas cuando forme parte de una denominación más amplia que requiera su uso. El acrónimo será (TIC) y deberá utilizase siempre en mayúsculas. DÍAZ REVORIO, J., *Los derechos humanos ante los…, op. cit.,* pp. 165-166.

informática, los ordenadores y las redes.[342] La suma de estos dos conceptos deriva en el concepto de TIC (TIC= TI +TC).

Un concepto general de TIC y, probablemente el que se debe entender en este trabajo, por la naturaleza jurídica y no informática, es el que se refiere a estas como el conjunto de tecnologías y servicios de comunicación e información. Estas tecnologías permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética. Podríamos decir, que tienen en común la electrónica, que es la que soporta los contenidos indicados.[343]

Los soportes electrónicos, a través de los cuales se transmite la información, también han evolucionado con el transcurso del tiempo (telégrafo óptico, teléfono fijo, celulares, televisión) y en la actualidad se suman la computadora e Internet. El uso de las TIC representa una variación notable en la sociedad y a la larga un cambio en la educación, en las relaciones interpersonales, en la manera de

---

[342] *Cfr.* DÍAZ REVORIO, J., *Los derechos humanos ante los…, op. cit.,* p. 166. *v. et.* Otra definición, y probablemente, las más acogida en los trabajos de investigación, es la ofrecida por el Programa de las Naciones Unidas para el Desarrollo (PNUD): *"Las TIC se conciben como el universo de dos conjuntos, representados por las tradicionales tecnologías de la comunicación (TC) - constituidas principalmente por la radio, la televisión y la telefonía - y por las tecnologías de la información (TI) caracterizadas por la digitalización de las tecnologías de registros de contenidos (informática), de las comunicaciones, (telemática) y de las interfaces (mediática), lo cual ha sido posible dada la adaptabilidad que ofrece la computación". Informe sobre desarrollo humano en Venezuela,* 2002. p. 9. Consultable en: http://hdr.undp.org/sites/default/files/venezuela_2002_es.pdf

[343] En ese sentido, Rosario, señala que: *"Las TIC incluyen la electrónica como tecnología base que soporta el desarrollo de las telecomunicaciones, la informática y el audiovisual"*. ROSARIO, J., *La tecnología de la información y la comunicación (TIC). Su uso como herramienta para el fortalecimiento y el desarrollo de la educación virtual,* 2005, disponible en el archivo del Observatorio para la CiberSociedad [en línea], http://www.cibersociedad.net/archivo/articulo.php?art=218

comunicarnos y de obtener información, así como en la forma de difundir y generar conocimientos, entre otros aspectos.[344]

Las TIC, así como tienen una gran cantidad de aplicaciones prácticas, tienen una gran cantidad de características. Expondremos solo algunas de ellas con el propósito de señalar las más importantes para delimitar, de alguna manera y si esto es posible, una cercanía a los conceptos que se han señalado.

[344] Uno de los primeros expositores sobre el impacto de Internet y las TIC en la sociedad fue Nicholas Negroponte en 1995 (fundador y director de Media Lab del MIT). Resaltó que las tecnologías hacen posible el desarrollo de sectores diferenciados de tecnologías para confluir hasta conformar un todo indiferenciable. En GARCÍA MEXÍA, P., "El Derecho de Internet", *op. cit.*, p. 121.

2.1. Inmaterialidad (Posibilidad de digitalización).

Las TIC convierten la información, tradicionalmente sujeta a un medio físico, en inmaterial. Mediante la digitalización es posible almacenar grandes cantidades de información en dispositivos físicos de pequeño tamaño (medios ópticos, magnéticos, electrónicos, etc.). A su vez, los usuarios pueden acceder a información ubicada en dispositivos electrónicos lejanos, que se transmiten utilizando las redes de comunicación, de una forma transparente e inmaterial.

Esta característica ha venido a definir lo que se ha denominado como "realidad virtual", esto es, realidad no real[345]. Mediante el uso de las TIC se están creando grupos de personas que interactúan según sus propios intereses, conformando comunidades o grupos virtuales. Nuevos espacios de interacción social se han creado y las personas interactúan y socializan en estos.[346]

---

[345] Durante mucho tiempo se ha llamado "realidad virtual" al resultado de los productos tecnológicos que dan una apariencia de realidad, sin embargo, en la actualidad el límite entre lo real y lo virtual se está reduciendo. Lo virtual ha pasado a ser parte de la sociedad y afecta a los individuos de formas tan reales como la realidad. En las noticias vemos como el *ciberbullying* (acoso tecnológico) afecta la psicología de las personas, incluso ha llevado a algunas hasta el suicidio. El *ciberbullying* es el uso de los medios telemáticos (Internet, telefonía móvil y videojuegos online principalmente) para ejercer acoso psicológico entre iguales. No se trata aquí del acoso o abuso de índole estrictamente sexual ni los casos en los que personas adultas intervienen. Puede consultarse en: http://www.ciberbullying.com/cyberbullying/

[346] Una de las redes sociales más populares es Facebook, sin embargo, nuevas redes sociales aparecen ante las posibles intromisiones en la intimidad de las personas, una de ellas y con un lanzamiento reciente y de mucho impacto es la denominada red social Ello, que entre las primera líneas que le definen asegura ser una red sin publicidad y que no venderá los datos personales a terceras personas. Con relación a esta red social, se puede consultar en: https://ello.co/wtf/post/about-ello. Incluso tal es la popularidad de la creación de redes, que varios programas y aplicaciones permiten crear redes pequeñas y privadas, entre grupos de familiares o de personas con ciertas características comunes o afines, como la amistad, el seguimiento de ciertos gustos o hábitos, empatías, etc.

2.2. Instantaneidad.

Podemos transmitir la información instantáneamente a lugares muy alejados físicamente, mediante las denominadas "autopistas de la información".

Como se ha indicado, se han acuñado términos como *ciberespacio*[347]*,* para definir el espacio virtual, no real, en el que se sitúa la información, al no asumir las características físicas del objeto utilizado para su almacenamiento, adquiriendo ese grado de inmediatez e inmaterialidad.

2.3. Aplicaciones Multimedia.

Las aplicaciones o programas multimedia han sido desarrollados como una interfaz amigable y sencilla de comunicación, para facilitar el acceso de todos los usuarios a las TIC. Una de las características más importantes de estos entornos es "*la interactividad",* posiblemente la característica más significativa. A diferencia de las tecnologías más clásicas (TV, radio) que permiten una interacción unidireccional, de un emisor a una masa de espectadores pasivos, el uso del ordenador interconectado mediante las redes digitales de comunicación, proporciona una comunicación bidireccional (sincrónica y asincrónica), persona-persona y persona- grupo. Se está produciendo, por tanto, un cambio hacia la comunicación entre personas y grupos que interactúan según sus intereses, conformando lo que se denomina "comunidades virtuales". El usuario de las TIC es, por tanto, un sujeto activo, que envía sus propios mensajes y, lo más importante, toma las decisiones sobre el proceso a seguir: secuencia, ritmo, código, etc.

---

[347] *Vid*. *Supra* cita 336, p. 185.

Otra de las características más relevantes de las aplicaciones multimedia, y que mayor incidencia tienen sobre el sistema educativo, es la posibilidad de transmitir información a partir de diferentes medios (texto, imagen, sonido, animaciones, etc.). Por primera vez, en un mismo documento se pueden transmitir informaciones multi-sensoriales, desde un modelo interactivo.[348]

Como se ha venido indicando, las TIC han introducido una serie de cambios en la sociedad, han influido en las más diversas disciplinas del ser humano y sus ámbitos de acción, la lista de esto podría ser interminable. En el marco jurídico, desde hace muchos años, los juristas se han preocupado por la influencia de estas tecnologías. Incluso se habla de "nuevos derechos" o "derechos emergentes" como producto casi directo del uso de tecnologías. El Derecho a la protección de datos fue producto de la creación de bases de datos electrónicas y con ello surgió el derecho a la autodeterminación informativa. Hace algunos años se empezó a hablar del derecho de Internet como un derecho humano básico y refería al ejercicio de algunos derechos fundamentales en la red. Este nuevo derecho ha sido incorporado en los textos constitucionales de algunos países y, principalmente, desarrollado en la jurisprudencia constitucional[349].

---

[348] ROSARIO, J., *op. cit. s.n.*; En junio del 2014, la empresa *Vapor Communications*, hizo la primera demostración de un dispositivo, denominado oPhone, capaz de transmitir olores a través de Internet y con una capacidad de crear más de 300.000 combinaciones. Estos instrumentos aumentarán las experiencias de los usuarios en Internet permitiendo el uso del olfato para mejorar la interacción con la utilización de aromas. Mensajes perfumados, *werables* y otras aplicaciones a esta tecnología ya se encuentran en desarrollo por parte de estas empresas. *V. et.* CRIADO, M. Á., "Con el oPhone ya puedes enviar aromas desde el móvil" en *El Mundo.es*, blog del 20 de junio de 2014, [en línea], http://www.elmundo.es/yodona/blogs/techtaciones/2014/06/20/con-el-ophone-ya-puedes-enviar-aromas.html

[349] Vid. *Infra* Apartado 5 de este Capítulo.

3. VULNERABILIDAD DE LA INTIMIDAD EN INTERNET.

En la actualidad, como consecuencia de los avances tecnológicos y, principalmente, por el uso de Internet, los derechos y libertades fundamentales se ven amenazados. Los derechos que se estiman más vulnerables son los ejercitados a través de esta red, como la libertad de expresión, el acceso a la información, la vida privada de las personas, el secreto de las comunicaciones y la protección de los datos de carácter personal.

El derecho a la intimidad se ve amenazado, en especial, con la proliferación de grandes bases de datos, que son generadas tanto por la infraestructura estatal como por el sector privado. Este temor ha contribuido a la creación de mecanismos jurídicos que pretenden regular y restituir cualquier daño o amenaza al derecho de intimidad. En lo que respecta a la protección de datos personales, algunos autores consideran que se trata del surgimiento de un derecho distinto al derecho a la intimidad y que debe ser considerado como un derecho autónomo, mientras que otros lo consideran parte del derecho de intimidad[350].

En un sentido utópico, el avance de la informática, debiera verse como una forma generadora de libertades, pues el poder de la técnica no debería engendrar el temor, sino la esperanza de que se alcanzará un mayor grado de desarrollo personal y profesional, un crecimiento en todos los sentidos, aunque resulte

[350] El derecho a la intimidad no nace como consecuencia de estas nuevas tecnologías, no son estas las creadoras de un nuevo derecho a la intimidad, sino que este ya existía y respondía a idénticos conceptos y parámetros generales, aunque las distintas concepciones políticas de los gobiernos dominantes, en muchos períodos de la historia del mundo, se encargaron de borrarlo. PIERINI, A., LORENCES V., TORNABENE, M. I., *Hábeas data. Derecho a la intimidad,* 2ª ed., Editorial Universidad, Buenos Aires, 2002, p. 222. Sobre el tema se pude consultar el Capítulo V *infra*.

imposible aceptar esa afirmación sin cierto escepticismo, se podría considerar la posibilidad de crear mecanismos de control para detener los abusos del poder.[351]

El tema de seguridad informática es un tema de actualidad y constante lucha[352]. Existen varias causas generadoras de problemas que afectan la seguridad de los usuarios en Internet ante lo cual se han implementado mecanismos, desde diversas áreas de especialidad, para controlar o prevenir asuntos relacionados con la seguridad de los usuarios. Sin embargo, los que posean la mejor tecnología serán capaces de concentrar la mayor cantidad de datos referidos a la intimidad de las personas y podrán constituirse como dictadores de sus actos[353], dado que tendrán los datos necesarios para ejercer la coacción y condicionar su actividad como amenaza.

Por supuesto, el concepto de intimidad tiene un significado distinto para cada persona. Hoy día quienes se dedican a la aplicación de la ley, abogados y jueces, cuando hablan de intimidad se refieren a un rango de condiciones y libertades. De otra parte, en el lenguaje común el término de *invasión a la privacidad* se refiere a

---

[351] GOMEZ NAVAJAS, J., *op. cit.,* p. 37.

[352] Varios autores advierten que la posesión de la tecnología, su aplicación y posible manipulación, y la intimidad de las personas representan la base el conflicto, de muy difícil resolución y cuestionan que, si se sobrepasa la noción de frontera política y geográfica, ¿qué fuerza tendrá el *hombre común* para enfrentarse a tanto poder concentrado y defender su intimidad? Ante ello plantean que será la búsqueda de un justo límite fronterizo aceptado y reconocido por todos el que determinará el reconocimiento de la información como fuente de conocimiento y el derecho a la intimidad de los individuos. PIERINI, A., LORENCES V., TORNABENE, M. I., *op. cit.,* p. 223.

[353] *Ibíd.*

distintas violaciones, algunas reales y otras imaginarias, pero que juntas forman un concepto de categorías ilustradas que dan contenido a este concepto[354].

Cuando una red privada se conecta a Internet es posible que no toda la información, contenida en ella, quiera ponerse a disposición del público. Y seguramente se querrá que la información disponible no sea manipulada ni destruida. Con esta información en Internet cualquier usuario dispone de un acceso mínimo a través del cual puede intentar realizar operaciones indebidas. Desgraciadamente hay muchos usuarios dispuestos a romper la seguridad de los sistemas. Muchos de ellos lo intentan simplemente por "diversión" pero otros lo hacen con la intención de obtener algún tipo de ventaja. Entre los más conocidos destacan los hackers que normalmente se limitan a dejar una señal de su hazaña en los sistemas invadidos y, los más dañinos, destruyen todo lo que pueden. Resulta curiosa que la idea de Internet naciera de un proyecto de DARPA[355] relacionado con el Departamento de Defensa de EE.UU. y que ahora ese mismo organismo sea uno de los blancos favoritos de hackers y crackers.[356]

En el "Libro Naranja" del Departamento de Defensa (DoD) de EE.UU.[357] se describen los requisitos de seguridad que debe cumplir un sistema, proporcionando una serie de criterios para evaluar el estatus en el que se encuentran. Esta

---

[354] ALLEN, ANITA L., *Unpopular Privacy: What must we hide?,* Oxfort University Press, New York, 2011, [versión para lector digital Kindle].

[355] *Vid.* Apartado siguiente *infra* sobre las generalidades de Internet.

[356] *Vid.* DE ANDRÉS BLASCO, J., "¿Qué es Internet?", en GARCÍA MEXÍA, P. (dir.), *Principios de Derecho de Internet, op cit.*, pp. 72-73. Al efecto señala: *"un sistema completamente seguro es aquel que se encuentra sin conexión a la red, apagado, desenchufado y metido dentro de una caja fuerte inexpugnable cuya combinación sólo conoce una persona que se murió el año pasado".*

[357] Department of Defense, *Trusted computer system evaluation criteria,* 1985, [en línea], http://csrc.nist.gov/publications/history/dod85.pdf

especificación data de 1985 y se ha tomado como estándar. En ésta publicación se establecen varios grados de defensa dependiendo del tipo de seguridad.

La preocupación por la intimidad y privacidad se han incrementado luego de casos como el de Snowden relacionado con la denuncia de la vigilancia masiva por el gobierno de los EE.UU.[358], particularmente, por la NSA. La utilización de nuevos medios de almacenamiento de información en la nube ha experimentado un considerable crecimiento por parte de los usuarios, sustituyendo los medios tradicionales de almacenamiento de archivos electrónicos. El avance en esas tecnologías ha ganado terreno y cada vez más se ofrecen nuevos servicios de alojamiento de archivos en servidores conectados a Internet, tecnología que irá en aumento dadas las ventajas que ofrecen los dispositivos que se conectan y utilizan esas tecnologías.

A partir de la masificación de Internet y algunos servicios de valor agregado, como buscadores, redes sociales, *webmail*, entre otros, el tema de la privacidad de la información comenzó a adquirir mayor trascendencia para la comunidad en general y no solo para los expertos del área de seguridad informática o las empresas. En 2004 fue posible observar que, junto con el lanzamiento de Gmail, el servicio de correo electrónico de Google, algunos usuarios se mostraron preocupados por la privacidad del mismo. La razón de esto se debe a que la empresa puede analizar el contenido del correo para mostrar publicidad que sea acorde a los intereses de las personas.[359]

---

[358] *Vid.* Sobre la vigilancia masiva Capítulo VI *infra*.

[359] Equipo de investigación de ESET Latinoamérica, *Tendencias 2014: El desafío de la privacidad en Internet,* 2014, [en línea], http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

Nuevas empresas con motores de búsqueda que no rastrean la información de los usuarios incrementaron las visitas luego de las revelaciones hechas por Snowden[360], una de ellas es la empresa DuckDuckGo[361], cuyo tráfico se incrementó en un 200%.[362] La tendencia global que se observa en la actualidad es hacia una mayor preocupación con respecto a cómo las empresas y los gobiernos almacenan, controlan y utilizan información privada de los usuarios en Internet.

Es posible que este caso haya contribuido a que muchas personas alrededor del mundo reflexionen, y a la vez se vean más interesadas, creando conciencia sobre la privacidad de sus datos en línea. Pese a esta preocupación y, más allá del extenso debate social y mediático que generó todo el tema de la NSA, las medidas de protección que adoptan los usuarios para resguardar la privacidad y seguridad de los entornos informáticos que utilizan (computadoras, teléfonos inteligentes, tabletas y otros) son, en muchas ocasiones, bastante deficientes. Asimismo, producto de la falta de conciencia y con exceso de confianza, las personas suelen actuar de un modo riesgoso con respecto a la seguridad de sus datos.

De acuerdo a documentos filtrados por Snowden, la presidenta de Brasil, Dilma Rousseff y el de México, Enrique Peña Nieto, fueron espiados y para ello interceptaron las llamadas telefónicas, correos electrónicos y mensajes de texto de la presidenta de Brasil y varios de sus asesores que fueron monitoreados por la

---

[360] Sobre las revelaciones de Edward Snowden se desarrolla en el Capítulo VI *infra* de esta investigación un análisis concreto en razón de la importancia y se exponen las reacciones incluso jurídicas que se iniciaron contra el gobierno de los EE.UU. por la posible vulneración del derecho a la intimidad de las personas.

[361] Buscador web *duckduckgo* en: https://duckduckgo.com/

[362] Sobre el tráfico de la página se puede consultar en: https://duckduckgo.com/traffic.html

NSA. En el caso de Peña Nieto, el espionaje se hizo cuando aún era candidato a la presidencia y se replicó, también, a nueve miembros de su equipo.[363]

La frase "*servida en charola de plata"* parece apropiada para estos casos, dado que así se entrega la información a las empresas privadas a cambio de algún servicio, para lo cual el usuario debe aceptar de manera previa las condiciones que se exigen para obtener el servicio, bastando un *click* para colocar una marca, mediante la cual acepta "voluntariamente" y por adhesión un contrato o cláusulas en las que se incluyen autorizaciones para utilizar la información, así como renuncias a la privacidad, reglas que en la mayoría de los casos ni siquiera se leen. De forma diaria los servicios contratados por medio de Internet y las aplicaciones utilizadas en el móvil, tienen acceso a datos personales. Con esa información en manos de los operadores de estos servicios es sumamente fácil hacer perfiles de los usuarios y deducir, con mucha precisión, otros datos, incluidos algunos considerados como sensibles.

El derecho de intimidad, a la confidencialidad de los datos de todas las personas, es un derecho fundamental y es necesario para que sean respetados como seres autónomos y libres, teniendo en cuenta que el cuerpo, la mente, los datos sociales y sanitarios forman parte de la intimidad, de la privacidad y de la confidencialidad de las personas.[364]

El derecho a la intimidad es necesario para que el individuo pueda desarrollar el derecho a de autonomía y, de esta forma, tomar por sí solo las decisiones que

---

[363] MIRANDA, L., "La NSA espió a los presidentes de Brasil y México" en *FayerWayer,* 02 de setiembre de 2013, [diario en línea], http://www.fayerwayer.com/2013/09/la-nsa-espio-a-los-presidentes-de-brasil-y-mexico/; *v. et.* MIGUEL, P., "El espionaje de EU se extendió a equipos de asesores de Rousseff y Peña Nieto" en *Periódico La Jornada*, 2 de setiembre de 2013, [en línea], http://www.jornada.unam.mx/2013/09/02/politica/013n1pol

[364] SÁNCHEZ CARAZO, C., "La protección de datos personales de las personas vulnerables", en *Anuario Facultad de Derecho*, Universidad de Alcalá II, 2009, p. 209, [en línea], http://dspace.uah.es/dspace/handle/10017/6443

mejor le convengan, siempre que no estén en juego derechos fundamentales de terceros o bienes y valores constitucionales, es decir, sin daño o menoscabo a los demás. El derecho a la vida privada es la autonomía, la libertad a que nadie disponga o imponga coactivamente lo que tengamos que hacer.

Dilma Rousseff, presidenta de Brasil, ha indicado en los medios de comunicación que su gobierno está tomando una serie de medidas contra el espionaje masivo del gobierno de los EE.UU. y la interceptación de comunicaciones del cual también ha sido víctima en lo personal. Al efecto indicó: *"habrá una creciente reacción de los países"* contra las prácticas de la NSA, porque cree *"que nadie, ninguna nación democrática, admitirá este quiebre de su soberanía y esta violación de los derechos humanos, de los derechos civiles de su población, que es lo que se hace a través de la NSA"*[365]

La aparición de nuevas técnicas de información y comunicación, de carácter digital, ha planteado el problema de determinar en qué medida el Derecho está preparado para hacer frente a tales retos. Una postura es la de quienes sostienen que, el advenimiento del mundo digital provoca la aparición de algunas características totalmente nuevas, que impiden tanto la aplicación de instrumentos jurídicos tradicionales como su adaptación al nuevo medio exigiendo, en consecuencia, una respuesta nueva por parte del Derecho.[366] Ese planteamiento resulta atendible si se estima que el enfoque tradicional puede ser compartible, pero la conclusión sería muy distinta si se admite en el estudio del Derecho la presencia

---

[365] KUMMETZ, P., "Dilma Rousseff: espionaje de EEUU es <inadmisible>", en *DW*, 24 de octubre de 2014, [en línea], http://www.dw.de/dilma-rousseff-espionaje-de-eeuu-es-inadmisible/a-17182013

[366] RUIZ MIGUEL, C., "Derechos constitucionales, fiscalidad e Internet: necesidad de una reformulación de conceptos tradicionales", en *Cuadernos Constitucionales de la Cátedra Fadrique Furió Ceriol*, Universitat de València, No. pp. 47-56.

de principios y reglas generales para la solución de los nuevos problemas y retos que plantean la utilización de estas nuevas tecnologías.

La globalización y transformaciones sociales, económicas, científicas y culturales han influenciado los derechos fundamentales. Magistralmente, lo apunta el profesor Díaz Revorio, al señalar que: *"Internet ocupa un papel protagonista y central en el ámbito de las nuevas tecnologías. Y por esta razón, hay algunas implicaciones específicas que suponen algunas peculiaridades de los derechos constitucionales cuando se ejercen a través de Internet o, en el extremo opuesto, son vulnerables o amenazados desde la red de redes"*.[367]

Se puede concluir que los derechos personales en general, principalmente aquellos que se ejercitan en Internet, resultan propensos a ser vulnerados por las nuevas tecnologías, dado su alcance y aparente falta de regulación. A ello se suman otros factores como la falta de educación, los intereses económicos, los intereses políticos y la capacidad de interconexión y convergencia, así como el desconocimiento de los afectados y su exceso de confianza al suministrar información ante las nuevas tecnologías.

Otros derechos nuevos o emergentes, surgen como respuesta al desarrollo tecnológico. Estos son los derechos de las sociedades electrónicas, que pretenden proteger las arbitrariedades del Estado y las empresas con relación a los derechos de quienes integran la sociedad del conocimiento.

---

[367] DÍAZ REVORIO, F.J., *Los derechos humanos ante…, op. cit.,* pp. *186-187.*

4. GENERALIDADES SOBRE INTERNET.

Para algunos autores, Internet es el espacio de la libertad, sobre todo para comunicar y expresarse, para desarrollar experiencias de investigación y culturales de cualquier tipo, trascendiendo las fronteras de los Estados.[368]

Cuesta imaginar que los orígenes de Internet se remontan al año de 1962, y en aquel entonces se utilizó el concepto de "red galáctica", que se refería a un conjunto de ordenadores interconectados globalmente, a través de los que todo el mundo podría acceder rápidamente a datos y programas desde cualquier sitio. Si bien el espíritu y el concepto resulta familiar con el Internet de hoy en día, lo cierto es que su funcionamiento distaba del que en la actualidad manejamos. Desde la creación del programa DARPA y el plan que se elaboró llamado ARPANET, tuvo que transcurrir tiempo significativo. Podría decirse que esta primera etapa incipiente pudo haber culminado en 1972 con la primera demostración pública de este instrumento que permitirá la transmisión de paquetes de datos, sin embargo, dichas transmisiones se limitaban al envío de mensajes de correo electrónico.

A partir de ese momento, el correo electrónico se convirtió en la aplicación de red más importante durante la década de los ochentas[369].

En los años ochenta la ARPANET se convirtió en Internet y para ese momento las dificultades que existían estaban relacionadas con los diversos y diferentes diseños de redes independientes que existían en esa fecha. Internet tal y como la conocemos hoy en día plasma una idea de una red de arquitectura abierta,

---

[368] Las propias tecnologías de la telecomunicación que se emplean en Internet están diseñadas de manera tal que, en ocasiones se hace imposible cualquier restricción a la libertad. MUÑOZ MACHADO, S., *La regulación de la red,* Taurus, Madrid, 2000, p. 151.

[369] INTERNET SOCIETY, *Breve historia de Internet,* 2012, [en línea], http://www.internetsociety.org/es/breve-historia-de-internet#Leiner

que permite una gran variedad de redes. En nuestros días no existen descripciones sobre el tipo de redes que se pueden incluir o sobre su alcance geográfico, aunque ciertas consideraciones pragmáticas dictaminan lo que tiene sentido ofrecer.

No conviene que se señale ahora que surgió primero, si los problemas con respecto al uso y actividad de Internet y su posterior regulación, o si, a raíz de esta regulación, iniciaron los primeros problemas. Lo cierto es que la inmaterialidad, la internacionalidad y la accesibilidad son características que, en conjunto con la centralización de control, han complicado la regulación universal del ciberespacio.

Se han realizado numerosos esfuerzos con el fin de establecer reglas universales en relación con el uso de Internet, pero lo cierto es que se está hablando de una dimensión cambiante, inmaterial, que no conoce fronteras de espacio y tiempo.

El surgimiento de Internet representa uno de los avances tecnológicos que más cambios ha producido, traduciéndose en el paso de la sociedad análoga a la sociedad digital.

Pero, ¿en qué consiste Internet y cuáles son sus implicaciones? Según algunas definiciones, Internet es un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos[370] TCP/IP[371],

---

[370] *Protocolo de Comunicación* es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.

[371] Se refiere al conjunto de protocolos de red en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de

garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Algunos definen Internet como “La Red de Redes”, y otros como “La Autopista de la Información”.[372]

En la actualidad Internet se presenta como un paso decisivo en el avance de los sistemas de información y comunicación a escala planetaria. Gracias a Internet cada ciudadano, sin moverse de su casa, puede acceder a los centros de documentación más importantes del mundo, puede realizar las más diversas operaciones financieras y comerciales, gozar de una enorme oferta de entretenimientos de la más diversa especie, y se puede comunicar con otros usuarios de la red sin limitaciones de número ni distancia. Si hace algunos años parecía que la “aldea global” era el gran reto del futuro, hoy Internet ha convertido en realidad presente el “hogar global”, en la medida en que cada domicilio de los usuarios de la red constituye la terminal de un sistema integrado de manera universal.[373]

Algunos autores han definido el ciberespacio como un microcosmos digital en el cual no existen fronteras, distancias ni autoridad centralizada. Los usos que se han dado a éstas tecnologías son muy variados. Diversas empresas comerciales han aprovechado esta nueva tecnología para ofrecer sus servicios a través de la red y algunas otras han creado nuevos servicios en función de esta. Uno de los

---

archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

[372] GARCÍA MEXÍA, P., “El derecho de Internet”, *op. cit.,* pp. 99-101.

[373] PEREZ LUÑO, A. E., “Impactos sociales y jurídicos de Internet” en *Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología,* No. 1, 1998, pp. 33-48, [en línea], http://www.argumentos.us.es/numero1/bluno.htm

servicios que más éxito ha tenido en Internet ha sido la World Wide Web[374] (WWW, o "la Web[375]"), hasta tal punto que es habitual la confusión entre ambos términos.

Existen muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia -telefonía (VoIP), televisión (IPTV)-, los boletines electrónicos (NNTP), el acceso remoto a otras máquinas (SSH y Telnet) o los juegos en línea.

La World Wide Web, o WWW como se suele abreviar, se inventó a finales de los 80 en el CERN[376] (Organización Europea para la Investigación Nuclear), el Laboratorio de Física de Partículas más importante del Mundo. Se trata de un sistema de distribución de información tipo revista. En la Red quedan almacenadas lo que se llaman Páginas Web, que no son más que páginas de texto con gráficos o fotos. Aquellos que se conecten a Internet pueden pedir acceder a dichas páginas y acto seguido éstas aparecen en la pantalla de su ordenador. Este sistema de visualización de la información revolucionó el desarrollo de Internet. A partir de la invención de la WWW, muchas personas empezaron a conectarse a la Red desde sus domicilios, como entretenimiento. Internet recibió un gran impulso, hasta el punto que, en la actualidad, cuando se habla de Internet, se refieren a la WWW.

El FTP (File Transfer Protocol) permite enviar ficheros de datos por Internet. Ya no es necesario guardar la información en disquetes para usarla en otro

---

[374] World Wide Web (WWW) es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet. Con un navegador Web, un usuario visualiza páginas web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.

[375] Web palabra que proviene del inglés y se refieren a una red o telaraña. Diccionario de la Lengua Española. Real Academia Española, 23ª ed., consultable en http://www.rae.es/rae.html

[376] CERN consultable en http://public.web.cern.ch/public/

ordenador. Con este servicio, muchas empresas informáticas han podido enviar sus productos a personas de todo el mundo sin necesidad de gastar dinero en miles de disquetes, ni envíos. Muchos particulares hacen uso de este servicio, por ejemplo, dar a conocer sus creaciones informáticas a nivel mundial.

Evidentemente, junto con esas incuestionables ventajas desligadas de las inmensas posibilidades de conocimiento, actuación y comunicación que permite la navegación por el ciberespacio, Internet ha hecho surgir en los últimos tiempos graves motivos de inquietud. La pornografía, la prostitución infantil, el narcotráfico, el terrorismo, violación a los derechos de autor, estafas y fraudes, etc. han sido sólo algunos de los temores sobre el peligro que representa el uso de esta tecnología. Sin embargo, esto no debe ser motivo de asombro, quienes han evaluado el impacto de la informática en las libertades, han alertado sobre sus peligros, y cualquier especialista mínimamente avisado incurriría en negligencia inexcusable de haberlos desatendido[377]. En las sociedades avanzadas con tecnología de punta ya no se puede juzgar como una amenaza remota las advertencias y experiencias de asalto informático a las libertades, que con el descubrimiento de los abusos perpetrados a través de Internet se han convertido en una siniestra realidad.[378]

Los expertos apuntan que Internet implica, un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos, con especial referencia a derechos como la intimidad, la imagen, la libertad sexual, la dignidad y el honor de

---

[377] PÉREZ LUÑO, A. E., "Impactos sociales y jurídicos de Internet" en *Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología*, No. 1, 1998, p. 131, [en línea], http://www.argumentos.us.es/numero1/bluno.htm

[378] *Ibíd.*

las personas; así como también afectaciones a bienes e intereses jurídicos como la propiedad intelectual e industrial y la seguridad nacional y el orden público.[379]

Internet plantea una preocupante paradoja, dado que por un lado muestra una eficacia global e ilimitada para atentar contra bienes y derechos, mientras que por el otro muestra una capacidad de respuesta jurídica fraccionada y limitada por las fronteras nacionales. Por ello, la reglamentación jurídica del flujo interno e internacional de datos es uno de los principales retos que hoy se plantean los ordenamientos jurídicos nacionales y las regulaciones internacionales.

El acceso a internet ha sido todo un desafío en los países del tercer mundo y ha generado lo que se conoce como "brecha digital"[380]. Mientras el acceso a Internet en algunos países o entre algunos sectores dentro de un mismo país es amplio e ilimitado, de alta velocidad y en óptimas condiciones tecnológicas, para otros este acceso es limitado ya sea por su condición socio-económica, por la educación que reciben o por residir en lugares en los cuales no se presta este servicio. Hay que indicar que existen diversas propuestas nacionales e internacionales para reducir la brecha digital.

Los orígenes o causas de la brecha digital, se atribuyen a distintas razones, entre ellas, la condición etaria, la educación, la condición socioeconómica, zonas

---

[379] RIBAS, J., *"*Aspectos legislativos de las autopistas de la información: Delitos en Internet*",* en *Jornadas Profesionales Informat- 96,* Barcelona, octubre, 1996, citado por PEREZ LUÑO, A. E., "Impactos sociales…", *op. cit.,* p. 131.

[380] El concepto de brecha digital se refiere a un término recientemente acuñado, el cual señala las diferencias en cuanto al acceso y uso de las aplicaciones de las tecnologías de información y comunicación (TIC) entre individuos de un mismo país, o entre diferentes países o regiones. MONGE, R., y CHACON F., *La Brecha Digital en Costa Rica. Acceso y uso de las Tecnologías de la Información y Comunicaciones (TIC's),* [en línea], http://www.caatec.org/CAATEC/publicaciones/crdigital/CR_Digital_1.pdf

urbanas o rurales y otros factores[381], sin embargo, el acceso a Internet ha sido creciente en todos los países, por ejemplo en España existen 4,1 millones de viviendas familiares que no disponen acceso a Internet, es decir, el 25,0% de los hogares españoles no cuentan con acceso a la Red[382].

En Costa Rica los números no son del todo alentadores, para el año 2012 (último censo) tenemos que un 47,3% de los hogares costarricenses tienen acceso a Internet y en su gran mayoría es por el acceso móvil, que cubre un 34%.[383]

---

[381] En un estudio de la Comisión Económica para América Latina y el Caribe (CEPAL) que data del año 2002, establece que la Brecha Digital Doméstica es, en esencia, un subproducto de las brechas socioeconómicas existentes en el respectivo país. Según la CEPAL, la tecnología digital en sí no es responsable de la brecha digital, sino que ésta es consecuencia de una serie de factores tales como el nivel de ingreso y su distribución, la dotación de la infraestructura de comunicaciones y el nivel de educación. El nivel de ingreso y su distribución está directamente relacionado con el costo de acceso a las tecnologías, es decir la tarifa mensual que debe pagar una persona, familia o empresa por el servicio de conexión, y que pueden tener varios componentes dependiendo del tipo de conexión. En este sentido, según el Global Competitiveness Report 2001-2002, varios de los países latinoamericanos tienen costos extremadamente elevados, lo que inhibe el acceso en los hogares. En estos casos, los negocios tipo cibercafés o las iniciativas colectivas como los telecentros se conviertan preferentemente en la alternativa viable para los ciudadanos. Informe *Hacia la sociedad de la Información y el Conocimiento en Costa Rica. La brecha digital en Costa Rica,* cap. 10, [en línea], http://www.gobiernofacil.go.cr/gobiernodigital/informes/cap10.pdf; Estudios más recientes como el primer avance de la medición de la Brecha Digital en Costa Rica 2009, en el cual se consignaron estadísticas sobre el acceso a los servicios de telecomunicaciones en Costa Rica y, en el 2010, surgió el Informe de avance del índice de Brecha Digital: Uso de las Tecnologías de Información y Comunicación, considerado como un primer esfuerzo para el establecimiento de un índice de Brecha Digital (IBD). Para el 2011, se investigó acerca del uso de los servicios de telecomunicaciones y se presentó el tercer avance de medición de dicha separación digital. El índice se basa en cuatro componentes que son el acceso, el uso, la calidad y la educación en tecnologías de la información y la comunicación (TIC). Así, de conformidad con el estudio realizado por la Rectoría de Telecomunicaciones en el año 2012, Costa Rica está ubicado para este año en un nivel de Brecha Digital media baja. *Cfr., Índice de Brecha Digital en Costa Rica,* Rectoría de Telecomunicaciones, 2011, p. 17-20, [en línea], http://www.telecom.go.cr/index.php/publicaciones/telecom/publicaciones/indice-de-brecha-digital-costa-rica/detail

[382] Centro de Investigaciones Sociológicas (CIS), barómetro de diciembre de 2014 (http://datos.cis.es/pdf/Es3047mar_A.pdf , pregunta 28.

[383] Instituto Nacional de Estadística, *Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los hogares 2014,* España, [en línea],

El Plan Maestro de Gobierno Digital 2011-2014, indica que Costa Rica tiene la tasa más baja de crecimiento de usuarios de Internet (700%) comparado con los países Latinoamericanos (1024%) entre el 2000 y el 2010.[384]

Para la disponibilidad de los servicios en línea existen criterios mundiales que evalúan el nivel alcanzado por los países producto de las iniciativas emprendidas. Para reducir la Brecha Digital es necesaria la participación de diversos sectores sociales a fin de articular esfuerzos para generar resultados a corto plazo. Según Muñoz Alvarado y Nicaragua Nicaragua, *"el gobierno debe orientar el sentido de entes como el Ministerio de Ciencia y Tecnología y el Consejo Nacional de Ciencia y Tecnología hacia una verdadera política de difusión de las TIC como herramientas para el desarrollo, labor a la que el Ministerio de Educación Pública se debe sumar con una verdadera enseñanza de competencias digitales más allá de las marcas de las aplicaciones"*[385]. Efectivamente, la participación del sector privado y las Universidades es trascendental para favorecer el desarrollo social y solidarios, con iniciativas que incluyan la participación democrática de las personas.

Se puede concluir que, desde el punto de vista de una sociedad democrática, la inclusión de las personas en una nueva sociedad electrónica e informatizada permite la participación ciudadana y el acceso a mejores oportunidades que permitirán mejorar la calidad de vida, reduciendo con ello las desigualdades que en un inicio han marcado de forma importante la creación de tecnologías que parecían

---

http://www.ine.es/jaxi/menu.do?type=pcaxis&path=/t25/p450/base_2011/a2014/&file=pcaxis; *v. et.*, VARELA FERRÍO, J., *La brecha digital en España estudio sobre la desigualdad postergada,* Comisión Ejecutiva Confederal de UGT, Madrid, 2015, [en línea], http://www.ugt.es/Publicaciones/BRECHADIGITAL_WEB.pdf

[384] Plan Maestro de Gobierno Digital 2011-2014, p. 18, [en línea] http://www.gobiernofacil.go.cr/E-GOB/gobiernodigital/informes/PlanMaestroGD.pdf

[385] MUÑOZ ALVARADO, M.D. Y NICARAGUA NICARAGUA, R., "Un acercamiento a la brecha digital en Costa Rica desde el punto de vista del acceso, la conectividad y la alfabetización digital" en evista electrónica publicada por la Escuela de Bibliotecología y Ciencias de la Información, UCR, vol. 4, No. 1, 2014, p. 22, [en línea], http://revistas.ucr.ac.cr/index.php/eciencias/article/view/12866/12328

reservadas a los sectores de la población con altos recursos económicos y altos grados de educación.

De esta manera, parece necesario recordar que la educación de las personas con respecto al uso de las tecnologías, debe incluir de forma necesaria la instrucción adecuada frente a los riesgos existentes y sobre todo al cuidado de la información personal y el respeto a la vida privada de otras personas.

5. ¿ES INTERNET UN DERECHO FUNDAMENTAL?

Desde el punto de vista de los derechos humanos, pareciera que Internet ha permitido el acceso efectivo a muchos de estos derechos, en este sentido la protección y regulación que se desarrolle respecto a su utilización requiere de una sensibilización especial y respeto absoluto por estos derechos.

El profesor Díaz Revorio señala que la incidencia de las nuevas tecnologías en los derechos fundamentales es amplia y compleja. Las TIC son un instrumento omnipresente en nuestra sociedad de información, en el seno de la cual ejercemos los derechos constitucionales. Por tanto, esta vinculación tan intensa por lo estrecho del vínculo, y al tiempo tan extensa por la amplitud de las implicaciones y relaciones existentes, entre TIC y derechos constitucionales, no es sino una manifestación de las relaciones entre Derecho y sociedad, y en particular una consecuencia de que los derechos constitucionales solo existen en tanto se ejercen en el seno de esta sociedad.[386]

La Directiva 2002/22/CE del Parlamento y del Consejo Europeo de 7 de marzo de 2002, podría considerarse como la primera norma jurídica en estimar Internet como un servicio funcional[387].

En igual sentido se puede estimar un reporte de la Organización para la Seguridad y la Cooperación en Europa (OSCE), que en un estudio revela que

---

[386] DIAZ REVORIO, F. J., *Los derechos humanos ante los…, op. cit.,* p. 171.

[387] Art. 4.2. de la Directiva 2002/22/CE del Parlamento y del Consejo Europeo de 7 de marzo de 2002, señala que *"La conexión proporcionada deberá permitir a los usuarios finales efectuar y recibir llamadas telefónicas locales, nacionales e internacionales, comunicaciones por fax y transmisiones de datos a velocidades suficientes para acceder de* ***forma funcional*** *a Internet, teniendo en cuenta las tecnologías dominantes utilizadas por la mayoría de los abonados y la viabilidad tecnológica".*

algunos gobiernos han tomado medidas legales para suspender el servicio en tiempo de guerra, estados de emergencia, desastres naturales, catástrofes, órdenes judiciales, incidentes de seguridad, límites de crédito del servicio, para la protección del sistema constitucional, protección de derechos de la propiedad intelectual o situaciones de seguridad nacional[388].

La organización de las Naciones Unidas ha calificado el acceso a Internet mediante dos iniciativas, como un derecho instrumental, como consecuencia de la libertad de expresión, lo cual indicó en un informe en mayo de 2011 de la Oficina del Alto Comisionado para los Derechos Humanos; y otra, más relevante y reciente, la Resolución del Consejo de Derechos Humanos de 5 de julio de 2012, en la cual indica que los mismos derechos que tienen las personas *offline* deben también protegerse *online*, en particular la libertad de expresión en Internet y en otras tecnologías, así como la forma en que Internet puede ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos[389].

Algunos gobiernos introdujeron en sus legislaciones el acceso a Internet como un derecho básico: entre los más relevantes, Estonia desde 2000, Grecia lo incluye como derecho constitucional desde el 2001, España y Finlandia desde 2003, Alemania desde 2004 y Turquía desde 2010[390].

---

[388] AKDENIZ, Y., "Freedom of Expression on the Internet", para la *Organization for Security and Co-operation in Europe (OSCE)*, Faculty of Law, Istanbul Bilgi University, Turkey, 2011, pp.39-40, [en línea], http://www.osce.org/fom/80723?download=true

[389] Naciones Unidas, Asamblea General, A/HRC/20/L.13 de 29 de junio de 2012, [en línea], http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

[390] GARCÍA MEXÍA, P., *Derechos y libertades, internet y tics*, Tirant lo Blanch, Valencia, 2014, p. 17.

Luego del reconocimiento de las Naciones Unidas en 2011, otros países se sumaron y reconocieron el acceso a Internet como un derecho instrumental derivado de la libertad de expresión: entre los casos más relevantes están el de Portugal, Rusia y Ucrania[391]. También destaca Francia, en el cual el Consejo Constitucional reconoció este derecho como un derecho humano básico, derivado de varios derechos, entre estos la libertad de expresión en el año 2009[392].

Así mismo, en España a través de la Ley 2/2011, de 4 de marzo[393], de economía sostenible, se introduce el derecho a acceso a Internet de banda ancha, estableciendo como mínimo una conectividad de 1 Mb/s para las descargas[394]. De igual manera, fue incluido en Finlandia un derecho similar en octubre de 2009[395].

---

[391] AKDENIZ, Y., "Freedom of Expression on the Internet", para la Organization for Security and Co-operation in Europe (OSCE), Faculty of Law, Istanbul Bilgi University, Turkey, 2011, pp.39-40, [en línea], http://www.osce.org/fom/80723?download=true

[392] Consejo Constitucional de la República francesa, sentencia número 2009/580 DC de 10 junio 2009, [en línea], http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009580DCes2009_580dc.pdf

[393] Art. 52, Ley 2/2011, de 4 de marzo, de economía sostenible, indica: *"Inclusión, como parte integrante del servicio universal, de una conexión que permita comunicaciones de datos de banda ancha a una velocidad de 1 Mbit por segundo"*.

[394] En España desde el mes de febrero de 2013, se implementó un programa de Agenda Digital para reducir la brecha digital y permitir mejores accesos a Internet. El Ministerio de Industria, Energía y Turismo y el Ministerio de Hacienda y Administraciones Públicas han liderado la elaboración de la Agenda Digital para España y han invitado al conjunto de agentes implicados a participar mediante un proceso abierto, transparente y colaborativo, [en línea], http://www.agendadigital.gob.es/Paginas/Index.aspx

MARTÍN, J., "El Gobierno pretende que en 2015 media España tenga Internet a 100 megas" en *El País,* 15 de febrero de 2015, [en línea], http://tecnologia.elpais.com/tecnologia/2013/02/15/actualidad/1360933452_238520.html

[395] AKDENIZ, Y., "Freedom of Expression on the Internet", *op. cit.,* pp. 39-40, [en línea], http://www.osce.org/fom/80723?download=true

En el año 2011, en los Países Bajos[396], se reguló por primera vez en Europa el derecho a disfrutar de una "Red Neutral", prohibiendo a los proveedores de servicios de Internet (ISP) bloquear o ralentizar el tráfico, salvo casos de seguridad nacional, congestión en las líneas o luchas contra el *spam* y otras prohibiciones relacionadas con facturaciones en razón de los servicios de aplicaciones suscritas por los usuarios.

Chile fue está considerado entre los primeros países en el mundo en introducir la protección de la neutralidad en la Red en el año 2010[397], mediante la Ley No. 20.453, que en su único artículo, propone modificaciones de varios artículos de la vigente Ley General de Telecomunicaciones, en las que se obliga a los proveedores de Red a "*no bloquear, interferir, discriminar, entorpecer ni restringir arbitrariamente el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal*".[398]

Sin embargo, en Costa Rica y con anterioridad, se contaba con dos precedentes legislativos de los cuales se puede inferir, claramente, el principio a la *neutralidad tecnológica*. El primero de ello contenido en la Ley de Firma Digital, Ley No. 8454, específicamente, en el artículo 2 inciso d) que señala como principio la "*Igualdad de tratamiento para las tecnologías de generación, proceso o almacenamiento involucradas*" y el segundo, se refiere a lo dispuesto en la Ley

---

[396] O'BRIEN, K.J., "Dutch Lawmakers Adopt Net Neutrality Law" en *The New York Times,* 22 de junio de 2011, [en línea], http://www.nytimes.com/2011/06/23/technology/23neutral.html?pagewanted=2&_r=2&partner=rss&emc=rss

[397] "Chile, primer país en incorporar la Neutralidad en la Red" en *Elmundo.es,* 16 de julio de 2010, [en línea], http://www.elmundo.es/elmundo/2010/07/16/navegante/1279272468.html

[398] Chile introduce en la Ley No. 20.453, el principio de neutralidad en la red para los consumidores y usuarios, consultable en línea, http://www.leychile.cl/Navegar?idNorma=1016570

General de Telecomunicaciones, Ley No. 8642, específicamente en el artículo 3 inciso h) que indica que uno de los principios es la "*Neutralidad tecnológica: posibilidad que tienen los operadores de redes y proveedores de servicios de telecomunicaciones para escoger las tecnologías por utilizar, siempre que estas dispongan de estándares comunes y garantizados, cumplan los requerimientos necesarios para satisfacer las metas y los objetivos de política sectorial y se garanticen, en forma adecuada, las condiciones de calidad y precio a que se refiere esta Ley*."

Uno de los argumentos del programa electoral de 2008 del actual presidente de los EE.UU., Barack Obama[399], fue la protección de la neutralidad en la red, en el cual proponía el acceso igualitario a las comunicaciones *online.* Nuevas propuestas de regulación fueron aprobadas en los EE.UU. desde el pasado 26 de enero de 2015[400], por parte de la Comisión Federal de Comunicaciones (*Federal Communications Commission* FCC[401]), en las cuales se estimó Internet como un servicio público. Ahora bien, para tales efectos, debió delimitarse, en este país, el servicio de Internet como un servicio de telecomunicaciones en lugar de un servicio de acceso a la información[402], situación que determinó la competencia legal de la

---

[399] *Vid.* BARACK, OBAMA, "Obama's Net Neutrality Plan" en *The New York Times,* 10 de noviembre de 2014, tomado de WhiteHouse.gov, [video en línea], http://www.nytimes.com/video/business/100000003226531/obamas-net-neutrality-plan.html?action=click&contentCollection=business&module=embedded&region=caption&pgtype=article

[400] *Federal Communications Commission* (FCC) Open Internet Order, 26 de enero de 2015, [en línea], https://www.fcc.gov/document/fcc-releases-open-internet-order

[401] Sobre la FCC se puede consultar en: https://www.fcc.gov/

[402] LOHR, S., "In Net Neutrality Push, F.C.C. Is Expected to Propose Regulating Internet Service as a Utility" en *The New York Times,* 2 de febrero de 2015, [en línea], http://www.nytimes.com/2015/02/03/technology/in-net-neutrality-push-fcc-is-expected-to-propose-regulating-the-internet-as-a-utility.html?ref=topics

FCC para emitir regulaciones y vigilar la actividad de la empresas ISP, desplazando la posición de tratar Internet como un servicio de información. En la jurisprudencia de este país, se habían sentado precedentes relacionados con respecto a la objetividad de los buscadores en línea, posibilitando a las empresas para controlar la información enviada a los usuarios, lo anterior basado en el derecho a la libertad de expresión[403].

Debe recordarse, que se había dado un fallo en enero de 2014[404] contra la Orden de Internet Abierta de la FCC por parte de las Corte de Apelaciones del Distrito de Columbia, que al igual que todas cortes de apelaciones federales de los EE.UU. sus fallos solo pueden ser revisados por parte de la Corte Suprema. En este fallo judicial, se rechazó el principio de neutralidad en Internet tal y como lo había planteado la FCC desde el año 2010[405].

Uno de los problemas con la utilización de Internet es el acceso a este servicio, esto ha sido todo un desafío en los países del tercer mundo y ha generado

---

[403] Al efecto se puede consultar en este Capítulo el apartado 6.4. *infra* sobre la neutralidad de los contenidos mostrados por los buscadores en Internet; *v. et.*, ROBERTS, J.J., "Google has free speech right in search results, court confirms", *Gigaom Research*, 17 de noviembre de 2014, [en línea], https://gigaom.com/2014/11/17/google-has-free-speech-right-in-search-results-court-confirms/; DANS, E., "Google y la libertad para manipular los resultados de búsqueda", *Blog Enrique Dans*, 18 de noviembre de 2014, [en línea], http://www.enriquedans.com/2014/11/google-y-la-libertad-para-manipular-los-resultados-de-busqueda.html

[404] *Vid.* Corte de Apelaciones del Distrito de Columbia, Verizon v. FCC, 740 F.3d 623, D.C. Cir. Jan. 14, 2014.

[405] Un estudio completo sobre la Orden de Internet Abierta de la FCC, puede consultarse en: https://www.fcc.gov/openinternet

lo que se conoce con el término de “brecha digital”[406], que proviene del inglés *digital divide*.

Según María Teresa Lugo[407], hablando de educación y acceso a las tecnologías, América Latina es la región más desigual y heterogénea del planeta. A pesar de haber evidenciado un crecimiento económico relativamente estable en las últimas dos décadas, muestra altos niveles de pobreza, de exclusión y de desigualdad social en amplios sectores de su población. Las mejoras importantes que en los últimos años se alcanzaron en una gran cantidad de aspectos no han sido suficientes para disminuir las brechas existentes -tanto internas como externas- ni para producir una reducción significativa de los niveles de pobreza.

El acceso Internet no es el único de los problemas que enfrentan las tecnologías de información y comunicación, existen muchos países en el mundo que cuentan con un excelente acceso a la red, sin embargo, estos accesos son restringidos. Estos límites a la libre navegación en Internet, producen una violación grosera de los derechos fundamentales de las personas, si bien es cierto que deben establecerse controles para la navegación en Internet, estos no pueden atender a razones políticas, religiosas, ideológicas o económicas.

Otro de los problemas graves, con relación al uso de tecnologías de información y comunicación, es la seguridad, particularmente la seguridad informática. Si bien es cierto se ha desarrollado normativa penal que sanciona conductas reprochables a través de medios telemáticos o informáticos, lo cierto es que entre más controles y seguridad tengamos más intimidad perdemos. Una de las

---

[406] *Vid.* *Supra* aparatado anterior de este Capítulo sobre el concepto de brecha digital.

[407] LUGO, M. T., *Las Políticas TIC en América Latina: prioridad de las agendas educativas,* 2015, [en línea], http://www.relpe.org/las-politicas-tic-en-america-latina-prioridad-de-las-agendas-educativas/

tareas o misiones que tenemos consiste en la búsqueda de soluciones que permitan mejorar la seguridad y respetar la intimidad.

Iniciativas internacionales y locales, así como algunas organizaciones de la sociedad civil han buscado diversas soluciones para mitigar, en alguna medida, los problemas que se han señalado con respecto al uso de Internet.

A altura se debería de interiorizar, profundamente, que Internet no tiene que ver con tecnología. Internet tiene que ver básicamente con la distribución democrática del capital informacional y con el acceso a la cultura y al saber. La brecha digital, íntimamente relacionada con la distancia entre ricos y pobres, desvirtúa el espíritu auténtico de esta tecnología y sienta las bases de una nueva forma de elitismo. El ataque a los derechos básicos de la persona y el aislamiento del sistema social son las consecuencias de esta nueva clase de analfabetismo[408].

Adicionalmente, existen problemas relacionados que no permiten un acceso efectivo a estas tecnologías, como lo son la falta de infraestructura de información y de telecomunicaciones, la cantidad de accesos a la información y el conocimiento, la educación y enseñanza del uso de estas tecnologías y la seguridad y condiciones propicias que fomenten un acceso igualitario para las personas.

Uno de los mejores esfuerzos, como se indicó *supra*, consiste en la declaratoria de acceso Internet como un derecho fundamental, que emitió el Consejo Constitucional de la República Francesa, en la sentencia número 2009/580 DC de 10 junio 2009, en la que repuntó como un derecho humano básico el acceso Internet, al desprenderlo, directamente, del artículo 11 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789, al sostener que: *"Considerando que de conformidad con el artículo 11 de la Declaración de los derechos del hombre y del ciudadano de 1789: «La libre comunicación de pensamientos y opiniones es*

---

[408] Internet Society. *op. cit. s.n.*

uno de los derechos más valiosos del hombre: cualquier ciudadano podrá, por consiguiente, hablar, escribir, imprimir libremente, siempre y cuando responda del abuso de esta libertad en los casos determinados por la ley»; que en el estado actual de los medios de comunicación y con respecto al desarrollo generalizado de los servicios de comunicación pública en línea así como a la importancia que tienen estos servicios para la participación en la vida democrática y la expresión de ideas y opiniones, este derecho implica la libertad de acceder a estos servicios."[409]

De otra parte, la Asamblea General de la Organización de Naciones Unidas, declaró el acceso a Internet como derecho humano altamente protegido. La ONU exigió a los países miembros que facilitaran servicio accesible y asequible para todos y estima como una prioridad, asegurar a la ciudadanía el acceso Internet. Señaló que tal reconocimiento no se trata solamente del derecho de opinión y de expresión, sino que también forma parte de sus derechos humanos y promueve el acceso de la sociedad en su conjunto, acceso que debe mantenerse especialmente en momentos políticos clave, elecciones, tiempos de intranquilidad social o adversarios históricos y políticos.

Podría concluirse que el acceso a Internet sigue siendo uno de los requisitos más importantes a efectos de ser parte e integrar la Sociedad de la Información. El acceso a Internet debería ser considerado como uno de los requisitos básicos del derecho a la libertad de expresión para difundir y recibir informaciones sin consideración de fronteras o límites de censura. De esta manera ese derecho es reconocido en el Reporte de la OSCE[410].

---

[409] Consejo Constitucional de la República Francesa, sentencia número 2009/580 DC de 10 junio 2009, [en línea], http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009580DCes2009_580dc.pdf

[410] AKDENIZ, Y., "Freedom of Expression on the Internet", *op. cit.,* p. 34, [en línea], http://www.osce.org/fom/80723?download=true

Se coincide en que todas las medidas jurídicas dictadas para regular el uso de Internet deben respetar los derechos y libertades fundamentales garantizados por los principios internacionales de los derechos humanos, especialmente la libertad de expresión y el flujo libre de información. Se hace necesario un trato neutral e igualitario con respecto a los servicios de Internet contratados por parte de las personas, no permitiendo las alianzas y estrategias comerciales que podrían acabar con grandes monopolios de empresas de comunicaciones e Internet.

Podría indicarse que es necesario que los esfuerzos para regulaciones mínimas en Internet deben implementarse a nivel internacional, mediante compromisos y la integración de la normativa local, lo anterior al evidenciarse la poca efectividad de las normas locales para regular el uso de los servicios *online.*

Países como Finlandia y Estonia consideran que el acceso a Internet es un derecho humano fundamental para los ciudadanos. Existen países que se oponen fuertemente a liberar el control de bloqueo sobre Internet, tal y como se había señalado al inicio de este apartado.

La Cumbre Mundial de la Sociedad de la Información (Ginebra 2003 – Túnez 2005)[411] señaló que existe un deseo y compromiso en común de construir, integrar y desarrollar una Sociedad de la Información centrada en la persona, en la cual las personas puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que los individuos, las comunidades y los pueblos puedan desarrollar su pleno potencial en la promoción de un desarrollo sostenible y mejorar su calidad de vida.

---

[411] Declaración de Principios para la primera fase de la Cumbre Mundial sobre la Sociedad de la Información, Ginebra, 10- 12 de diciembre 2003, [en línea], http://www.itu.int/wsis/docs/geneva/official/dop-es.html

6. INTIMIDAD EN INTERNET.

El uso de tecnologías, en la sociedad de la información y, principalmente, la informática, han permitido que, con mucha facilidad se puedan rastrear, almacenar, manipular, casar, cruzar, utilizar y transmitir piezas de información de las personas, piezas de información denominadas por los juristas "*datos personales*" que pueden en mayor o menor medida y, dependiendo del uso y finalidad, incidir de forma negativa en la intimidad, el secreto de las comunicaciones, el honor, la libertad sindical, la libertad religiosa o cualquier otro derecho fundamental, así como en otros derechos o intereses protegidos por el Ordenamiento. Hablar de tecnología informática y, sobre todo, de *Internet* es hablar del mayor escaparate de datos jamás conocidos, así como de la principal amenaza para la seguridad de estos[412].

[412] GARCÍA MEXÍA, P., "Internet y protección de datos. Los desafíos de la evolución digital", *Diario La Ley*, año XXXII, No. 7577, 25 de febrero de 2011, pp. 11-14.

6.1. Cookies HTTP.

El término de *Cookies de HTTP* se refiere a los datos almacenados en el ordenador de un usuario para ayudar al acceso de páginas web, pero también son utilizadas para el seguimiento o rastreo de las actividades de los usuarios. Sin lugar a dudas representan una preocupación para el ámbito de la intimidad de las personas. En principio no todas las *cookies* son utilizadas para fines ilegítimos[413], pero siempre se dan abusos, pues con estas se pueden identificar los hábitos de navegación de los internautas.

Uno de las empresas que aprovechó la utilización de las cookies ha sido Google, con el servicio de *Google Analytics*[414], servicio que genera informes sobre seguimiento y tráfico en Internet. Luego de que Google adquirió, en el año 2005, la empresa *Urchin Software Corp*., inició el servicio de Google Analytics, a través del cual puede hacer un seguimiento de la actividad de los usuarios en Internet. Este servicio ha planteado problemas de privacidad, sin embargo, los navegadores de Internet ahora brindan opciones para impedir el seguimiento.

Gran parte de la inversión en Internet se hace desde el sector de la publicidad online. Como es sabido, una de las formas en que la publicidad en Internet se lleva

---

[413] Uno de los beneficios podría ser que, para los sitios web que se visitan con frecuencia no se requiere introducir, nuevamente, una contraseña. Una cookie también puede realizar un seguimiento de las preferencias de los usuarios para mostrarles los sitios web que podrían interesarles. Pero, algunos de estos beneficios también son vistos como negativos. Por ejemplo, una de las formas más comunes de robo por parte de los hackers es cuando toman el nombre del usuario y la contraseña que salva una cookie. Una gran cantidad de sitios son de acceso libre, pero para poder obtener alguna ganancia o mantener los costos de operación venden su espacio a los anunciantes. Estos anuncios, que son personalizados a los propios gustos, a menudo pueden congelar la computadora o causar molestias.

[414] Más detalles del servicio de Google Analytics, puede ser consultado en: http://www.google.co.cr/intl/es/analytics/

a cabo es a través de las *cookies*. Las *cookies* son herramientas que tienen un papel esencial para la prestación de numerosos servicios de la sociedad de la información que concentran la mayor inversión publicitaria, facilitan la navegación del usuario y ofrecen una publicidad basada en ocasiones en los hábitos de navegación[415].

Uno de los problemas que planteaba la utilización de estos programas era, en principio, que no se informaba a los usuarios sobre la implementación de estas en las páginas web, situación que fue advertida mediante la Directiva 2009/136/CE del Parlamento Europeo y el Consejo del año 2009[416], que modificó la Directiva 2002/22/CE, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) No. 2006/2004 sobre la cooperación en materia de protección de los consumidores.

---

[415] Agencia Española de Protección de Datos (AEPD), "Guía sobre el uso de cookies", [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

[416] Esta Directiva, señala en el considerando 66 lo siguiente: "*Puede que haya terceros que deseen almacenar información sobre el equipo de un usuario o acceder a información ya almacenada, con distintos fines, que van desde los fines legítimos (como algunos tipos de cookies) hasta aquellos que suponen una intrusión injustificada en la esfera privada (como los programas espía o los virus). Resulta, por tanto, capital que los usuarios reciban una información clara y completa cuando realicen una acción que pueda dar lugar a dicho almacenamiento u obtención de acceso. El modo en que se facilite la información y se ofrezca el derecho de negativa debe ser el más sencillo posible para el usuario. Las excepciones a la obligación de facilitar información y proponer el derecho de negativa deben limitarse a aquellas situaciones en las que el almacenamiento técnico o el acceso sean estrictamente necesarios con el fin legítimo de permitir el uso de un servicio específico solicitado específicamente por el abonado o usuario. Cuando sea técnicamente posible y eficaz, de conformidad con las disposiciones pertinentes de la Directiva 95/46/CE, el consentimiento del usuario para aceptar el tratamiento de los datos puede facilitarse mediante el uso de los parámetros adecuados del navegador o de otra aplicación. La aplicación de estos requisitos debe ganar en eficacia gracias a las competencias reforzadas concedidas a las autoridades nacionales*".

Así mismo, la señalada normativa advierte sobre los programas informáticos que controlan subrepticiamente las acciones de los usuarios o que subvierten el funcionamiento de sus equipos terminales en beneficio de un tercero (spyware o "programas espía"), suponen una grave amenaza para la privacidad de los usuarios, como pueden ser los virus. Debe garantizarse un nivel de protección elevado e igual de la esfera privada de los usuarios, con independencia de si los programas espía no deseados o los virus se descargan inadvertidamente a través de las redes de comunicaciones electrónicas o se hallan ocultos en programas informáticos distribuidos en otros medios externos de almacenamiento de datos, como CD, CD-ROM, DVD, BLURAY o dispositivos de almacenamiento USB. Los Estados miembros deben fomentar el suministro de información a los usuarios finales sobre las precauciones disponibles y alentarlos a adoptar las medidas necesarias para proteger sus equipos terminales contra virus y programas espía[417].

En lo que respecta al almacenamiento de información por medio de *cookies,* el apartado segundo del artículo 22 de la LSSI[418] establece:

"2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Cuando sea técnicamente posible y eficaz, el

---

[417] *Vid.* Directiva 2009/136/CE del Parlamento Europeo y el Consejo del año 2009.

[418] Ley de servicios de la sociedad de la información y de comercio electrónico 34/2002, reformada por el Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista (en adelante, LSSI).

consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones, siempre que aquél deba proceder a su configuración durante su instalación o actualización mediante una acción expresa a tal efecto. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario."[419]

De conformidad con el precepto transcrito, este aplica a cualquier "dispositivo de almacenamiento y recuperación de datos" en cualquier "equipo terminal del destinatario" y que el Anexo de la citada LSSI define como "Destinatario del servicio o destinatario" a la "persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información".

Los desarrolladores de las cookies pretenden que sólo el sitio web que originalmente distribuye las cookies a los usuarios puedan recuperarlos. Sin embargo, en la práctica, los programadores pueden eludir esta restricción cuyas consecuencias podrían ser: a) la colocación de una etiqueta de identificación personal en un navegador para facilitar perfiles web o, b) el uso de *cross-site scripting* (XSS)[420] u otras técnicas para robar información de las cookies de un usuario.

---

[419] El artículo 22 de la LSSI se refiere a la instalación de cookies y tecnologías similares utilizadas (tales como local *shared objects*, *flash cookies*, etc.) para almacenar y recuperar datos de un equipo terminal (por ejemplo, un ordenador, un teléfono móvil o un tablet) de una persona física o jurídica que utiliza, un servicio de la sociedad de la información.

[420] XSS es un tipo de vulnerabilidad informática que afecta la seguridad. Permite a los atacantes introducir secuencias en los comandos de los usuarios de las páginas web para eludir controles de acceso, en español se conoce con el nombre de Secuencias de órdenes en sitios cruzados. Al efecto se puede consultar la página del Instituto Nacional de Ciberseguridad INCIBE de España, https://www.incibe.es/vulnSearch/CERT/Alerta_Temprana/Actualidad_Vulnerabilidades/buscador_vulnerabilidades/ayuda_buscador_vulnerabilidades/?postAction=getVulns

En muchas ocasiones los accesos a servicios o páginas web puede conllevar la instalación de ficheros o archivos en sus equipos terminales, y que al ser recuperados con la información almacenada en los mismos permiten, no sólo mejorar la navegación y prestar correctamente el servicio solicitado, sino que también posibilitan, con las implicaciones para la privacidad de los usuarios que ello supone, la recogida actualizada y continuada de datos relacionados con sus equipos y perfiles de navegación, que posteriormente podrán ser utilizados por los responsables de los sitios web a los que se accede, o por los terceros, para analizar su comportamiento y para el envío de publicidad basada en el mismo o como medio para el desarrollo de otros productos y servicios concretos. Por lo anterior, la normativa exige que en estas ocasiones se solicite el consentimiento informado a los usuarios para asegurar que tengan la información sobre el uso de sus datos y las finalidades para las cuales serán utilizados[421].

Existen diversas categorías de Cookies, como las de seguimiento, cookies de flash y las cookies zombies (evercookies). Los navegadores modernos pueden detectar y bloqueas este tipo de cookies.

En el documento citado, sobre la guía para la utilización de cookies[422], se clasifican por la tipología de la siguiente manera: a) Según la entidad que las gestione; b) Según el plazo de tiempo que permanecen activadas; y, c) Según su finalidad.

---

[421] *Vid.* Resolución R/01676/2015 de la Agencia Española de Protección de Datos (AEPD), [en línea], http://www.agpd.es/portalwebAGPD/resoluciones/procedimiento_apercibimiento/procedimiento_apercibimiento_2015/common/pdfs/A-00119-2015_Resolucion-de-fecha-01-07-2015_Art-ii-culo-22.2-LSSI.pdf

[422] Agencia Española de Protección de Datos (AEPD), "Guía sobre el uso de cookies", [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

6.1.1. Según la entidad que las gestione:

Según quien sea la entidad que gestione el equipo o dominio desde donde se envían las *cookies* y trate los datos que se obtengan, se puede distinguir dos tipos, las propias y las de terceros.

- ***Cookies* propias:** Son las enviadas al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el cual se presta el servicio solicitado por el usuario.
- ***Cookies* de tercero:** Son las enviadas al equipo terminal del usuario desde un equipo o dominio el cual no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos través de las *cookies*. En el caso que las cookies sean instaladas desde un equipo o dominio gestionado por el propio editor, pero la información que se recoja mediante estas sea gestionada por un tercero, no pueden ser consideradas como cookies propias.

6.1.2. Según el plazo de tiempo que permanecen activadas:

Según el plazo de tiempo que permanecen activadas en el equipo terminal podemos distinguir dos tipos, las de sesión y las persistentes.

- ***Cookies* de sesión:** Son un tipo de cookies diseñadas para recabar y almacenar datos del usuario para acceder a una página web. Se suelen emplear para almacenar información que solo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión (*e.g.* una lista de productos adquiridos).
- ***Cookies* persistentes:** Son un tipo de cookies en las cuales los datos siguen almacenados en el terminal y pueden ser accedidos y tratados durante un periodo definido por el responsable de la *cookie*, y este plazo puede ser de unos minutos a varios años.

6.1.3. Según su finalidad:

Según la finalidad para la cual se utilizan los datos obtenidos a través de las *cookies,* podemos distinguir entre las técnicas, de personalización, de análisis y las publicitarias.

- ***Cookies* técnicas:** Son las que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan (*e.g.* como controlar el tráfico y la comunicación de datos, identificar la sesión, acceder a partes de acceso restringido, recordar los elementos que integran un pedido, realizar el proceso de compra de un pedido, realizar la solicitud de inscripción o participación en un evento, utilizar elementos de seguridad durante la navegación, almacenar contenidos para la difusión de videos o sonido o compartir contenidos a través de redes sociales).
- ***Cookies* de personalización:** Son las que permiten al usuario acceder al servicio con algunas características generales predefinidas en función de una serie de criterios en el terminal del usuario (*e.g.* como el idioma, el tipo de navegador a través del cual accede al servicio, la configuración regional desde donde accede al servicio, etc.).
- ***Cookies* de análisis:** Son las que permiten al responsable de las mismas, el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas. La información recogida mediante este tipo de cookies se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma y para la elaboración de perfiles de navegación de los usuarios de dichos sitios, aplicaciones y plataformas, con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.
- Respecto al tratamiento de datos recabados a través de las *cookies* de análisis, se estima que, a pesar de que no están exentas del deber de obtener un consentimiento informado para su uso, es poco probable que

representen un riesgo para la privacidad de los usuarios siempre que se trate de cookies de primera parte, que manejen datos agregados con una finalidad estrictamente estadística, que se facilite información sobre sus uso y se incluya la posibilidad de que los usuarios manifiesten su negativa sobre su utilización.

- ***Cookies* publicitarias:** Son las que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios que, en su caso, el editor haya incluido en una página web, aplicación o plataforma que incluye la que presta el servicio solicitado en base a criterios como el contenido editado o la frecuencia en la que se muestran los anuncios.
- ***Cookies* de publicidad comportamental:** Son las que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios que, en su caso, el editor haya incluido en una página web, aplicación o plataforma desde la que presta el servicio solicitado. Estas *cookies* almacenan información del comportamiento de los usuarios, obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo.

En todos los supuestos en los cuales se utiliza la tecnología de *cookies,* y este conlleva la utilización de datos personales, los responsables de tal tratamiento deberán asegurarse del cumplimiento de las exigencias adicionales establecidas por la normativa sobre protección de datos personales, en particular en relación con los datos especialmente protegidos. Todas la *cookies* que no utilicen datos personales, como las de entrada del usuario, autenticación o identificación de usuario (únicamente de sesión), seguridad del usuario, reproductor multimedia, sesión para equilibrar la carga, personalización de la interfaz de usuario y

complemento (plug-in) para intercambiar contenidos sociales, están excluidas de las regulaciones normativas relacionadas con la protección de datos personales[423].

[423] Agencia Española de Protección de Datos (AEPD), “Guía sobre el uso de cookies”, [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

6.2. Proveedores de Internet ISP.

Los proveedores de servicios de Internet por sus siglas en inglés (ISP), por lo general son compañías que se dedican a las telecomunicaciones y brindan los servicios de acceso a Internet. Se estima que, al controlar la prestación de estos servicios, estas empresas podrían convertirse en vigilantes de las actividades de los usuarios en línea.

A modo de ilustración, el acceso a Internet se encuentra protagonizado por los siguientes agentes: a) Proveedor de acceso a Internet (Internet Access Provider, IAP), que a través de la red de acceso (distribuida en nodos de acceso, Points of Presence, POPs), conecta a los usuarios finales con el Proveedor de Servicios de Internet (ISP). b) Proveedor de Servicios de Internet (ISP), que conecta con Internet a los usuarios a través de la red y de los puntos de acceso (Net Access Points, NAPs) del IAP. c) Proveedor de contenidos, que genera información en forma de páginas Web, vídeo, audio, noticias, etc. d) Servicios de Internet: alojamiento de distintos servicios o hosting (correo electrónico, WWW, canales de noticias, etc.), mediante alquiler de capacidad de los servidores y de las comunicaciones. e) Proveedor de circuitos alquilados: suministro de la infraestructura de transporte para la conexión a Internet de los ISP y de los grandes usuarios. f) Concentradores de tráfico de Internet y operadores con la llamada “espina dorsal” (Backbone) de Internet[424].

Una gran variedad de datos pasan a través de los ISP, en algunos casos esos datos están encriptados. El HTTPS es unos de los cifrados más populares

[424] GARCÍA MEXIA, P. y CORONA HERRERO, U., “Internet y el derecho de las telecomunicaciones: El régimen jurídico del acceso a la Red” en GARCÍA MEXÍA, P. (dir.), *Principios de Derecho de Internet*, Tirant lo Blanch, Valencia, 2a ed., 2005, p.160.

utilizados en la actualidad para el envío de información. Si bien los proveedores de servicios de Internet podrían colectar los datos de los usuarios, lo normal es que se colecten datos relacionados con el objetivo de la conexión, como por ejemplo los relacionados con las direcciones IP y la información de la facturación.

El paso de la información a través de los proveedores de internet, podría ser utilizado para la prevención de delitos o la localización de criminales[425]. En Internet, los usuarios tienen asignada una dirección IP[426], que es una etiqueta numérica que les identifica. Adicionalmente, a través de esta dirección, también es posible realizar la geolocalización[427].

Es posible que el paso de la información a través de un ISP no sea una de las afrentas más intensas al derecho de intimidad, sin embargo, siempre existe la posibilidad de que esta información pueda ser utilizada de forma arbitraria en perjuicio de los usuarios. Existen diversas formas de enmascarar la dirección IP, lo cual es utilizado por los criminales informáticos para evadir la persecución.

---

[425] En México, se propuso una reforma en el Código Penal Federal, para la persecución de delitos de pornografía infantil, en el cual se propone la colaboración de las empresas proveedoras del servicio de Internet. PANSZA, A., "Proveedores de servicios de Interne podrían ser sancionados si no denuncian materia pornográfico", en *La Prensa,* 8 de setiembre de 2014, [en línea], http://www.oem.com.mx/laprensa/notas/n3531399.htm

[426] *Internet Assigned Numbers Authority* (IANA) es la organización responsable de la coordinación global del Protocolo de Internet (IP) frente a los sistemas, así como los Número de Sistemas Autónomos utilizados para enrutar el tráfico de Internet. Actualmente, hay dos tipos de protocolo de Internet (IP) en uso: IP versión 4 (IPv4) y versión 6 (IPv6). Al efecto puede consultarse en la página de la organización: https://www.iana.org/numbers

[427] En Internet existen muchos servicios que brindan la información de las direcciones IP que utilizan los ordenadores o dispositivos. Al efecto se puede consultar Geo IP Tool en: https://www.geoiptool.com/

6.3. Información biométrica e imágenes.

La biométrica se refiere a la identificación de personas a partir del reconocimiento de rasgos físicos, rasgos conductuales[428] o la combinación de ambos. La medida única de las huellas digitales, análisis de la imagen del dedo; reconocimiento del iris, análisis de la retina, reconocimiento facial, resultado de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, análisis de las muestras de ADN y análisis de los poros de la piel hacen posible la distinción automatizada de los seres humanos. Esta tecnología es muy útil para la prevención de fraudes[429] y la protección de los ordenadores frente a accesos no autorizados, pues se puede asegurar la identidad de las personas.

La utilización de huellas dactilares para diferencias personas, fue utilizado por primera vez por un policía francés, Alphonse Bertillon[430], quien en 1883 aplicó este sistema para identificar a criminales, de ahí que el sistema antropométrico se le denominara Bertillonage.[431]

---

[428] La biometría también permite utilizar datos sobre el comportamiento de las personas, como la comprobación de la firma manuscrita, la pulsación sobre las teclas, la forma de caminar, etc.

[429] La empresa TheatMetrix realizó un informe en el cual detectó de octubre de 2014 a marzo de 2015, más de 11.4 millones de intentos de fraude de suplantación de identidad, [en línea], http://info.threatmetrix.com/WP-2015Q1CybercrimeReport_WP-LP.html

[430] Alphonse Bertillon, fue un criminólogo y antropólogo francés que creó el primer sistema de mediciones físicas para identificar delincuentes, al efecto se puede consultar en: http://www.all-about-forensic-science.com/alphonse-bertillon.html

[431] Al efecto se puede consultar el Estudio sobre las tecnologías biométricas aplicadas a la seguridad del INTECO, [en línea], file:///C:/Users/Andres/Desktop/informe_biometria_final.pdf

El elemento biométrico de las personas puede ser: a) universal, cuando existe en todas las personas. b) único, cuando es distintivo para cada persona. c) permanente, cuando la simetría se mantiene a lo largo del tiempo para cada persona. También se suele distinguir entre datos biométricos estáticos y los datos biométricos dinámicos.

El uso de estas tecnologías de identificación da prioridad a los datos biométricos estáticos, por cuanto su margen de error es casi nulo en comparación con los datos biométricos dinámicos, lo cuales no garantizan la fiabilidad[432]. Tanto los datos biométricos estáticos como, los dinámicos refieren aspectos personales de todo individuo puesto que redundan en la esfera privada de estos; aunque algunos de estos datos biométricos, dependiendo de su naturaleza, son más cercanos que otros a esa esfera íntima del individuo.

Los *datos biométricos* al proceder de rasgos físicos o biológicos de las personas y dado que permiten determinar su identidad y elaborar un perfil, tienen protección jurídica. En sentido general la protección jurídica de los datos biométricos en el ámbito europeo está determinada por la Directiva 1995/46/CE[433] sobre protección de datos de carácter personal, al considerarse estos datos como datos personales. Las disposiciones señaladas en esa normativa quedan limitadas, en su

---

[432] TAPIA BUENO, S. G., "La Protección Jurídica de los Datos Biométricos en la Comunidad Europea", agosto, 2005, [en línea], http://www.buscalegis.ufsc.br/revistas/files/anexos/5548-5540-1-PB.htm

[433] El artículo 2.a) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre del 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, define datos personales como *"toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*.

radio de acción, cuando el uso de los datos biométricos tengan como finalidad cuestiones relacionadas a la seguridad de los Estados miembros de la Unión[434].

La huella dactilar, así como otros datos biométricos, son considerados como datos personales. Al efecto, la LOPD[435], en el artículo 3 a) define los datos de carácter personal como "*cualquier información concerniente a personas físicas identificadas o identificable*", de otra parte, el Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, en el artículo 5.1 f) señala como dato personal "Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". En el artículo 5.1 o) se señala que será identificable "*toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados*".

Algunos datos biométricos, por su naturaleza, son considerados como datos sensibles[436], y por ello no deben ser objeto de tratamiento externo, puesto que tienen "*incidencia con el ámbito más íntimo y personal de las personas, cuyo tratamiento puede incorporar peligro, no sólo de discriminación, sino de que sean*

---

[434] TAPIA BUENO, S. G., *op. cit.,* [en línea], http://www.buscalegis.ufsc.br/revistas/files/anexos/5548-5540-1-PB.htm

[435] Ley Orgánica 15/1999, de 13 de diciembre, sobre la Protección de Datos de Carácter Personal de España.

[436] El artículo 8.1 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre del 1995, prohíbe el tratamiento de este tipo de datos considerados "sensibles" por las informaciones que revelan.

conocidos por terceras personas a las que no queremos hacer partícipes de unos datos íntimos"[437].

Uno de los datos biométricos que puede ser catalogado de sensible es aquel que tiene que ver con la *imagen*. La plantilla biométrica de un reconocimiento facial puede evidenciar el origen étnico o racial de una persona y esto es considerado también por la Directiva 95/46/CE como un dato sensible.

De igual forma y con una consideración especial, los datos genéticos son protegidos dependiendo del análisis de ADN que se haga, si es del ADN codificante o no codificante, será considerado sensible o no ese dato biométrico, por la importancia que esto reviste[438].

Los datos genéticos se encuentran protegidos de forma especial, en la normativa europea. En ese sentido se ha regulado la utilización de datos genéticos en el Convenio para la protección de los Derechos Humanos y la Dignidad del Ser Humano, con respecto a las aplicaciones de la biología y la medicina o también llamado Convenio relativo a los Derechos Humanos y la Biomedicina, elaborado por el Consejo de Europa, del 4 de abril de 1997 y la Declaración Universal sobre el Genoma Humano y los Derechos Humanos de la UNESCO, del 16 de noviembre del 1999.

Evidentemente, la protección frente al tratamiento externo de los datos sensibles, como derecho fundamental, tampoco es absoluta. En la normativa aplicable se indican las excepciones del principio de prohibición de tratamiento de datos sensibles y estas consisten: en que el titular de los datos otorgue su

---

[437] FREIXAS GUTIERREZ, G., *La Protección de Datos de Carácter Personal en el Derecho Español*, Editorial Bosch, Barcelona, 2001, pág. 127.

[438] TAPIA BUENO, S. G., *op. cit.,* [en línea], http://www.buscalegis.ufsc.br/revistas/files/anexos/5548-5540-1-PB.htm

consentimiento para que otras personas tengan acceso a ellos o que, por razones de interés público, preservación del propio titular o de otras personas, para la prevención o diagnóstico médico, entre otras, se pueda disponer del tratamiento externo de los datos biométricos sin el consentimiento del titular.

6.4. Motores de búsqueda.

Los motores de búsqueda de Internet son comúnmente utilizados para encontrar las páginas Web y podernos desplazar entre estas. Estos motores tienen la capacidad de almacenar la información de los usuarios para personalizar las búsquedas, acelerarlas y refinarlas en razón de los intereses de los usuarios. Para esto, utilizan cookies de rastreo, cuentas de usuarios y registran las direcciones IP, sin embargo, no todos los buscadores utilizan estas cookies de rastreo.

La intimidad y la privacidad se ven afectadas con la utilización de la mayoría de programas de búsqueda, pues permiten, como se indicó, la creación de perfiles de usuarios, información que tiene un alto valor comercial para las empresas, las cuales a partir de ella pueden determinar los hábitos de consumo de las personas, entre otras cosas.

A modo de ejemplo, se puede recordar que, en el año 2006, la empresa AOL publicó de forma accidental el historial de más de 650.000 usuarios. Si bien esta base de datos no incluía el nombre o identidades de los usuarios, pues en su lugar se le asigna un número por parte de la empresa, sin embargo con los datos relacionados de las búsquedas podrían descubrir con facilidad la identidad de las personas[439].

Existen una gran cantidad de buscadores en Internet con distintas funciones, entre los más populares, se tienen: Google, Yahoo!, Boodigo, Bing, Wólfram Alpha, Alexa, Foofind, Qihoo 360, Ccsearch, Duckduckgo, Chacha, Yacy, Carrot, Hakia, Baidu, Open Directory Project, Blekko, Accoona, Yandex, Sohu, Gennio, Wotbox.Com. También existen Metabuscadores como: Kartoo, Ask Jeeves, Hakia, Sogou, Metacrawler, Gigablast, Ixquick, Apocalx, Yippy, Wikia Search y

[439] McCULLAGH, D., “AOL's disturbing glimpse into users' lives” en *CNET,* 7 de agosto de 2006, [en línea], http://www.cnet.com/news/aols-disturbing-glimpse-into-users-lives/

Webcrawler. Cada uno de estos buscadores y metabuscadores poseen características distintas, que responden en alguna medida a las búsquedas que realizan los usuarios.

Dado que los buscadores son generadores de información importante de las personas y dada la necesidad que se tiene para utilizarlos, se plantea una pequeña referencia de las más importantes, en razón de la cantidad de usuarios o la protección de la intimidad que pretenden algunos.

Google (www.google.com)**:** sin duda alguna es el buscador más conocido, su éxito depende en buena medida de la posibilidad de procesar cantidades inmensas de información. Google recibe un aproximado de 780.000.000 de visitas diarias[440], en febrero de 2015 se realizaron 17.000.000.000 de búsquedas con Google Sites[441].

Bing (www.bing.com): es el buscador oficial de Microsoft, sus nombres anteriores eran Live Search, Windows Live Search y MSN Search. Al igual que Google, permite las búsquedas personalizadas y relacionadas de acuerdo con las preferencias del usuario.

Yahoo! (www.yahoo.com): otro motor de búsqueda personalizada, a febrero de 2015, ocupa el tercer lugar luego de Google y Bing[442].

---

[440] Dato tomado de www.alexa.com

[441] Puede consultarse el informe de la empresa comScore, del 17 de marzo de 2015, sobre la utilización de buscadores en Internet, [en línea], http://www.comscore.com/Insights/Market-Rankings/comScore-Releases-February-2015-US-Desktop-Search-Engine-Rankings

[442] *Ibíd.*

Ixquick (www.ixquick.com): es el buscador de la empresa ixquick.com, que también ofrece los servicios de búsqueda en Internet sin el rastreo y la copia de las direcciones IP. En la publicidad del motor de búsqueda, señala que: *"Esas búsquedas revelan una impresionante cantidad de información personal sobre usted, como sus intereses, circunstancias familiares, inclinación política, afecciones médicas y más. Esta información vale oro para vendedores, funcionarios del gobierno, piratas informáticos y criminales, a quienes les encantaría apoderarse de su información de búsqueda privada."* [443] Con esas razones, la empresa ofrece un servicio libre de rastros del buscador.

Otros de los buscadores que no almacenan información de los usuarios son DuckDuckGo, Starpage, Gibiru, Lukol, MetaGer (Alemania), Ecosia y Disconnect Search. Otros motores como el de la empresa Seeks o Yacy, utilizan tecnologías *peer to peer* que, permiten realizar búsquedas en Google, Bing, Yahoo, Blekko de forma anónima.

Probablemente una de las situaciones jurídicas más relevantes respecto de los motores de búsqueda ha sido la sentencia del Tribunal de Justicia Europeo relacionada con la empresa Google, en la cual se determinó la responsabilidad de los gestores de motores de búsqueda con respecto al tratamiento de los datos de carácter personal que aparecen en las páginas web publicadas por terceros. En esta sentencia, el Tribunal señaló: *"que al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda "recoge" tales datos, en el sentido de la Directiva 95/46/CE. El Tribunal de Justicia estima, además, que dicho gestor "extrae", "registra" y "organiza" esos datos en el marco de sus programas de indexación, antes de "conservarlos" en sus servidores y, en su caso, los "comunica" a sus usuarios y les*

---

[443] IXQUICK.COM, "Ixquick Protege Su Privacidad", [en línea], https://ixquick.com/esp/protect-privacy.html?hmb=1, en la publicidad de la empresa se señala que, "*desde enero de 2009, ya no registramos las direcciones IP de nuestros usuarios*".

"facilita el acceso" a los mismos en forma de listas de resultados. Estas operaciones, mencionadas en la Directiva de forma explícita e incondicional, deben calificarse de "tratamiento", con independencia de que el gestor del motor de búsqueda las aplique de modo indiferenciado a informaciones que no son datos personales. Por lo demás, el Tribunal de Justicia recuerda que las operaciones a las que se refiere la Directiva también deben calificarse de "tratamiento" aun cuando sólo se refieran a información ya publicada, tal cual, en los medios de comunicación. Si en este último caso se estableciera una excepción general a la aplicación de la Directiva, esta última quedaría en gran medida vacía de contenido"[444].

En esa sentencia, el Tribunal determinó que la empresa del motor de búsqueda era responsable del tratamiento de los datos y los equiparó a las actividades de los editores de sitios de Internet, por cuanto el tratamiento de esos datos puede afectar, significativamente, los derechos fundamentales de respeto de la vida privada y de protección de los datos personales. El gestor del motor de búsqueda debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que dicha actividad satisfaga las exigencias de la Directiva. Sólo así las garantías establecidas en dicha norma podrán tener plenos efectos y podrá hacerse realidad la protección eficaz y completa de los interesados (y en particular de su derecho al respeto de la vida privada)[445].

Un análisis sobre los alcances y la efectividad de la sentencia es planteado *infra* en el apartado sobre la protección jurídica de los datos personales en el Capítulo V.

---

[444] Tribunal de Justicia de la Unión Europea, Comunicado de prensa No. 70/14, Luxemburgo, 13 de mayo de 2014, [en línea], http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070es.pdf, la sentencia completa puede ser consultada en: http://curia.europa.eu/juris/documents.jsf?num=C-131/12

[445] *Ibíd.*

Otro de los problemas que se han planteado relacionado con los motores de búsqueda, es la selección del contenido a mostrar, es decir, muestran la información de forma selectiva a los usuarios pues muestran la que ellos consideran apropiada según sus propios criterios selectivos y según los intereses comerciales que manejen al respecto. Las búsquedas de los motores son consideradas como publicaciones, por lo cual se respaldan en la libertad de expresión y no tienen la obligación jurídica de brindar la información de forma objetiva, neutral o completa. La Corte de San Francisco EE.UU., ha dado la razón al Google al ampararle con la primera enmienda (libertad de expresión) para manipular los resultados de las búsquedas, al considerar que la puede organizar como mejor le convenga[446].

[446] ROBERTS, J.J., "Google has free speech right in search results, court confirms", *Gigaom Research*, 17 de noviembre de 2014, [en línea], https://gigaom.com/2014/11/17/google-has-free-speech-right-in-search-results-court-confirms/; DANS, E., "Google y la libertad para manipular los resultados de búsqueda", *Blog Enrique Dans*, 18 de noviembre de 2014, [en línea], http://www.enriquedans.com/2014/11/google-y-la-libertad-para-manipular-los-resultados-de-busqueda.html

6.5. Redes sociales.

Se conoce como redes sociales[447] los servicios *on-line* prestados a través de Internet que permiten a los usuarios generar un perfil público, en el cual plasman datos personales e información, disponiendo de herramientas que les permiten interactuar con el resto de usuarios afines o no al perfil publicado[448].

Una red social es una estructura social en la que hay individuos y existen relaciones de distinto tipo entre ellos. Al aparecer de los sitios web que brindan la funcionalidad de interconectar personas, nacen las redes sociales virtuales. Las redes sociales presentan un medio ideal para conectarse con amigos y posibles socios comerciales, pero también para la averiguación de datos[449].

Las redes sociales tienen su fundamento en la teoría de los seis grados de separación (Six Degrees)[450], según la cual cualquier individuo puede estar conectado a otra persona del planeta, a través de una cadena de conocidos con no más de cinco intermediarios (seis conexiones). La cifra de conocidos aumenta a medida que lo hacen los eslabones de la cadena. Los individuos de primer grado

---

[447] Debe advertirse que, en la doctrina, no existe un concepto cerrado y aceptado de forma unitaria.

[448] Sobre las redes sociales consúltese la página de la AEPD y el Instituto Nacional de Tecnologías de la Comunicación (INTENCO), "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online", 2009, [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

[449] GUERRA VALDIVIA, A. R., "Redes Sociales" en NAVA GARCÉS, Alberto (coord.), *El derecho en la era digital*, ed. Porrúa, México, 2013, [versión para lector digital Kindle].

[450] Teoría inicialmente propuesta en 1929 por el escritor húngaro Frigyes Karinthy. Recogida también en el libro "Six Degrees: The Science of a Connected Age" del sociólogo Duncan Watts, quien asegura que es posible acceder a cualquier persona del planeta en tan solo seis "saltos".

serán los más próximos y, según se avanza en el grado de separación, disminuye la relación y la confianza.

Desde la puesta en marcha de la Web 2.0[451], los perfiles sociales han causado una creciente preocupación para la privacidad en Internet. Este servicio ha facilitado el intercambio de información participativa y la colaboración de Internet en redes sociales[452] a través de sitios como Facebook, Instagram, Twitter y MySpace[453], los cuales se han convertido en aplicaciones muy populares. Con estas aplicaciones, los usuarios "suben" información personal a la red.

Este tipo de redes se ha convertido en un medio poderoso de comunicación e interacción[454], permitiendo a los usuarios el ocio, hacer negocios o practicar el

---

[451] El concepto de "Web 2.0" comenzó con una sesión de "brainstorming" realizada entre O'Reilly y MediaLive International en el año 2004. Dale Dougherty, pionero de la web y vicepresidente de O'Reilly, observó que lejos de "estrellarse" y decaer, la web era más activa que nunca, con apasionantes nuevas aplicaciones y con sitios web apareciendo con sorprendente regularidad. Un sitio Web 2.0 permite a los usuarios interactuar y colaborar entre sí como creadores de contenido generado por usuarios en una comunidad virtual.

[452] Las llamadas redes sociales online consisten en servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el cual plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado. GONZÁLEZ FREA, L., "Aspectos Legales y Normativos de las Redes Sociales", [en línea], http://www.gonzalezfrea.com.ar/derecho-informatico/aspectos-legales-redes-sociales-legislacion-normativa-facebook-regulacion-legal-argentina/265/

[453] Ejemplos de otros servicios que permite la Web 2.0 son las comunidades web, los servicios web, servicios de red social, de alojamiento de video, wikis, blogs, mashups y folcsonomías. En el año 2002 comienzan a aparecer sitios web que promocionan las redes de círculos de amigos en línea, adquiriendo popularidad en el año 2003 con la llegada de portales web como MySpace o Xing.

[454] A nivel mundial, las últimas estadísticas (3ª Oleada del Estudio Power to the people social media, Wave 3 de Universal McCann de marzo 2008) cifran el número de usuarios de redes sociales en 272 millones, un 58% de los usuarios de Internet registrados en todo el mundo, lo que supone un incremento del 21% respecto de los datos registrados en junio de 2007. AEPD e Instituto Nacional de Tecnologías de la Comunicación (INTENCO), "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online", 2009, [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

comercio, obtener o difundir noticias, brindar o enterarse de opiniones, participar en organizaciones, realizar su actividad profesional entre muchas otras actividades, teniendo un gran impacto en la sociedad.

Se estima que el aumento de popularidad de las redes sociales transcurre en paralelo al aumento en los niveles de intercambio de contenidos a través de la Red. Es posible que ello propiciara que Internet se transformara en un medio más social al permitir comunicar, entretener y compartir.

Los usuarios han pasado de una etapa en la que eran considerados meros consumidores de contenidos creados por terceros usuarios con ciertos conocimientos de programación, a una etapa en la que los contenidos son producidos por los propios usuarios equipados con un ordenador, conexión y conocimientos básicos en el uso de Internet[455].

Con la aparición de los servicios que ofrece la web 2.0, los usuarios se han convertido en participantes y creadores de contenidos e información, dejando atrás y superando el rol de observadores.

6.5.1. Clasificación de las redes sociales.

Las redes sociales podrían dividirse en dos tipos: a) las análogas o redes sociales *off-line,* que son aquellas en las cuales las relaciones se desarrollan sin mediación de sistemas electrónicos, con independencia del medio empleado y; b) las digitales o redes sociales *on-line,* las que se originan a través de medio digitales

[455] AEPD e Instituto Nacional de Tecnologías de la Comunicación (INTENCO), "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online", 2009, [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

o electrónicos[456]. Sin embargo, ambas tienen en común que se trata de una forma de la interacción entre miembros y/o espacios sociales.

Según la propuesta realizada por Burgueño[457], las redes sociales digitales o redes sociales *on-line,* se pueden clasificar:

6.5.1.1. Por su público, objetivo y temática, en redes horizontales y verticales:

- **Redes sociales Horizontales:** aquellas dirigidas a todo tipo de usuario y sin una temática definida. Se basan en una estructura de celdillas permitiendo la entrada y participación libre y genérica sin un fin definido, distinto del de generar masa. Los ejemplos más representativos del sector son Facebook, Orkut, Identi.ca, Twitter.
- **Redes sociales Verticales:** están concebidas sobre la base de un eje temático agregador. Su objetivo es el de congregar en torno a una temática definida a un colectivo concreto. En función de su especialización, pueden clasificarse a su vez en: verticales profesionales (Viadeo, Xing y Linked In), verticales de ocio (Wipley, Minube, Dogster, Last.FM y Moterus) y verticales mixtas (Yuglo, Unience, PideCita, 11870).

6.5.1.2. Por el sujeto principal de la relación:

- **Redes sociales Humanas:** son aquellas que centran su atención en fomentar las relaciones entre personas, uniendo individuos según su perfil social y en función de sus gustos, aficiones, lugares de trabajo, viajes y

---

[456] BURGUEÑO, P., "Clasificación de las Redes Sociales", *Blog personal de Pablo Burgueño,* 2 de marzo de 2009, [en línea], http://www.pabloburgueno.com/2009/03/clasificacion-de-redes-sociales/; *Cfr.* GUERRA VALDIVIA, A. R., "Redes Sociales" en NAVA GARCÉS, Alberto (coord.), *El derecho en la era digital*, ed. Porrúa, México, 2013, [versión para lector digital Kindle].

[457] *Ibíd.*

actividades. Ejemplos de este tipo de redes los encontramos en Dopplr y Tuenti.

- **Redes sociales de Contenidos:** las relaciones se desarrollan uniendo perfiles a través de contenido publicado, los objetos que posee el usuario o los archivos que se encuentran en su ordenador. Los ejemplos más significativos son Scribd, Flickr, Bebo, Dipity, StumbleUpon y FileRide.
- **Redes sociales de Objetos:** conforman un sector novedoso entre las redes sociales. Su objeto es unir marcas, automóviles y lugares. Entre estas redes sociales destacan las que rinden tributos a las personas fallecidas, es un lugar social en el que familiares y amigos rinde homenaje a personas que ya no están en vida. El ejemplo más llamativo es Respectance.

6.5.1.3. Por su localización geográfica:

- **Redes sociales Sedentarias:** este tipo de red social muta en función de las relaciones entre personas, los contenidos compartidos o los eventos creados. Ejemplos de este tipo de redes son: Blogger, Plaxo, Bitacoras.com, Plurk.
- **Redes sociales Nómadas:** a las características propias de las redes sociales sedentarias se le suma un nuevo factor de mutación o desarrollo basado en la localización geográfica del sujeto. Este tipo de redes se componen y recomponen a tenor de los sujetos que se hallen geográficamente cerca del lugar en el que se encuentra el usuario, los lugares que haya visitado o aquellos a los que tenga previsto acudir. Los ejemplos más destacados son: Foursquare, Latitude, Fire Eagle y Skout.

6.5.1.4. Por su plataforma:

- **Red Social MMORPG y Metaversos:** normalmente construidos sobre una base técnica Cliente-Servidor (WOW, SecondLife, Lineage,

Gladiatus, Travian, Habbo). Son juegos de multijugadores en línea, generalmente juegos de roles para caracterizar un personaje ficticio.

- **Red Social Web:** su plataforma de desarrollo está basada en una estructura típica de web. Algunos ejemplos representativos son: MySpace, Friendfeed y Hi5.

6.5.2. Intimidad en las redes sociales.

Tal y como se mencionó, en las redes sociales los usuarios facilitan una serie de datos de carácter personal al inscribirse en estos portales, que deben ser convenientemente protegidos en la legislación. La naturaleza de este tipo de servicios promueve que los usuarios incluyan amplia información sobre sus preferencias y necesidades[458].

El Grupo Internacional sobre protección de datos en las Telecomunicaciones de Berlín aprobó, en su reunión del 4 de marzo de 2008, el "*Rome Memorandum*"[459]. En él se destaca que *"uno de los desafíos que pueden observarse es que la mayoría de la información que se publica en las redes sociales, se hace bajo la iniciativa de*

[458] Sobre los riesgos de la privacidad en las redes sociales, se puede consultar el documento de la European Network and Information Security Agency (ENISA) publicado en octubre de 2007, sobre "Recomendaciones y seguridad para las redes sociales online" dirigido tanto a los proveedores de redes sociales como a los órganos encargados de dictar normas al respecto, en el que se realizan una serie de recomendaciones, entre las que se destaca la inversión en educación de los usuarios de estas redes o la promoción de mayores controles de acceso y autenticación, [en línea], https://www.enisa.europa.eu/publications/archive/soc-net; así mismo, se puede consultar el documento relacionado con cuestiones de seguridad de las redes sociales, en el cual se resaltan las amenazas más importantes y las recomendaciones de acciones y prácticas para reducir los riesgos de seguridad de los usuarios, publicado en noviembre de 2007, [en línea], http://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks

[459] Report and Guidance on Privacy in Social Network Services, "Rome Memorandum", [en línea], http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

los usuarios y basado en su consentimiento", se analizan los riesgos para la privacidad y seguridad de las redes sociales, y se apuntan unas pautas a los reguladores, a los proveedores y a los usuarios. En este documento se establece además que la aparente gratuidad de los servicios no se da siempre, dado que los usuarios, de hecho, pagan a través de usos secundarios con sus perfiles personales, como puede ser el marketing dirigido o personalizado[460].

Una de las principales críticas que ha recibido Facebook, la red social más importante, ha sido a falta de intimidad, críticas que aumentaron luego de las revelaciones de Edward Snowden en el año 2013 sobre la vigilancia que realiza la Agencia de Seguridad Nacional NSA en los perfiles de los usuarios.

Según lo informado por Snowden, desde el año 2010 la NSA ha estado explorando las enormes cantidades de datos para crea sofisticados gráficos de conexiones sociales de los estadounidenses, identificando sus asociados, ubicaciones, compañeros y cualquier otra información personal, los cuales incluyen el análisis de las llamadas telefónicas y registros de correos electrónicos[461].

Teniendo en consideración las cantidades de información que manejan las redes sociales, relacionado con los servicios de intercambio de información y comunicación, se tiene, además, información de carácter personal, la cual es de acceso público y global.

---

[460] AEPD e Instituto Nacional de Tecnologías de la Comunicación (INTENCO), "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online", 2009, [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

[461] RISEN J., "N.S.A. Gathers Data on Social Connections of U.S. Citizens", *The New York Times,* 28 de setiembre de 2013, [en línea], http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?src=mv&_r=1

Se pueden identificar dos momentos[462] en los cuales se pone en riego la privacidad de las personas al utilizar las redes sociales: a) en el momento en el cual se da de alta en el servicio, y; b) en el momento en el cual se participa como usuario de la red social.

En el primer caso se deben mencionar los contratos electrónicos para hacer uso de estos servicios, los cuales, si bien tienen un apartado completo sobre las políticas de privacidad, la mayoría de los usuarios no reparan en determinarlos, por lo cual optan por aceptar las condiciones del contrato de adhesión. Además, en este punto, el usuario por lo general no configura las opciones de privacidad del servicio, las cuales, en muchas ocasiones, por defecto, se encuentran en el modo más público. De otra parte, en el segundo caso, los usuarios, aunque de forma voluntaria han accedido a participar en redes sociales, podrían desconocer el alcance de sus publicaciones, afectando con ello su propia intimidad o la de terceras personas. Además, en algunos casos si no se aceptan las políticas y condiciones ya fijadas por la empresa u organización que maneja el programa, no es posible darse de alta o utilizarlo.

La Agencia Española de Protección de Datos se ha pronunciado sobre los alcances de las publicaciones en redes sociales, con respecto a los datos personales de terceras personas. En ese sentido se pronunció sobre la actuación de un centro educativo que publicó la foto de una menor en Facebook sin el consentimiento de sus padres. En esas diligencias, si bien se estimó la infracción

---

[462] GONZÁLEZ FREA, L., *op. cit.*, [en línea], http://www.gonzalezfrea.com.ar/derecho-informatico/aspectos-legales-redes-sociales-legislacion-normativa-facebook-regulacion-legal-argentina/265/ *Cfr*. AEPD e Instituto Nacional de Tecnologías de la Comunicación (INTENCO), "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online", 2009, [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

de los artículos 6.1 y 10 de la LOPD, se utilizó un criterio con el cual aplicaron medidas correctivas en lugar de una sanción, de conformidad con lo dispuesto en el artículo 45.6 de la citada ley, puesto que ante la solicitud de los padres retiraron la foto de la menor y dado que alegaron se trataba de un error con relación al consentimiento solicitado[463].

Se debe considerar que la mayoría de las redes sociales permite a los motores de búsqueda de Internet, indexar todos los contenidos de los perfiles de los usuarios, incluida la personal y la de los contactos[464]. Pareciera que los usuarios suelen olvidar el hecho de que se trata de herramientas públicas[465] y accesibles para cualquier tipo de persona, con independencia de las intenciones con las que se accede sean negativas o ilícitas.

Se estima que las redes generalistas o de ocio, son más propensas a riesgos de privacidad que las redes de tipo profesional, puesto que los usuarios no solo exponen sus datos, sino que se pueden exponer de manera pública las vivencias,

---

[463] Resolución R/01116/2015 de la AEPD, [en línea], http://www.agpd.es/portalwebAGPD/resoluciones/procedimiento_apercibimiento/procedimiento_apercibimiento_2015/common/pdfs/A-00055-2015_Resolucion-de-fecha-13-05-2015_Art-ii-culo-6-LOPD.pdf. En lo que respecta a la protección de menores de edad e incapaces, en el Real Decreto 1720/2007 se introduce una importante especialidad sobre la prestación del consentimiento por parte de estos menores al disponer que para recabar los datos de cualquier menor de 14 años es necesario contar con el consentimiento de los padres o tutores.

[464] AEPD e Instituto Nacional de Tecnologías de la Comunicación (INTENCO), "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online", 2009, [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

[465] Un estudio del año 2008 sobre "Redes Sociales Análisis cuantitativo y cualitativo sobre hábitos, usos y actuaciones" publicado por Ofcom (Office of Communications) afirma que casi la mitad de los usuarios de redes sociales analizados (44%) tienen su perfil de usuario sin restricciones de privacidad y disponible para que pueda ser visitado por cualquier otro usuario, [en línea], http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf

gustos, ideología y experiencias del usuario, lo que conlleva que el número de datos de carácter personal puestos a disposición del público sea mayor que en las redes sociales de tipo profesional. Asimismo, se tratan datos especialmente protegidos, lo que supone un mayor nivel de riesgo para la protección de dichos datos personales y, por ende, del ámbito de la privacidad e intimidad de los usuarios[466].

[466] AEPD e Instituto Nacional de Tecnologías de la Comunicación (INTENCO), "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online", 2009, [en línea], http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

6.6. Big Data y la Revolución Industrial 4.0.

La Revolución Digital o Cuarta Revolución Industrial es el nombre con el cual se denomina al cambio de la tecnología análoga, mecánica y electrónica a la tecnología digital. El comienzo de esta revolución ha marcado una nueva era, la Era de la Información.

En la actualidad se vislumbra una cuarta revolución, la Revolución de la "fábrica inteligente" o Industria 4.0, la cual se refiere al desarrollo del software, sistemas masivos de datos (*Big Data*) y su almacenamiento, la incorporación de sensores y electrónica a los elementos que interactúan en los procesos productivos y en los productos derivados de ellos, la convivencia hombre-máquina y la disponibilidad de la información enriquecida para una mejor y más acertada toma de decisiones[467].

El desarrollo de programas informáticos, con la posibilidad de analizar grandes cantidades de datos y la gestión de este conocimiento, se está volviendo un factor determinante en las organizaciones. En particular, las empresas de TI están implementando sistemas *Big Data*[468]*,* sistemas capaces de dar salida a grandes cantidades de datos procedentes del entorno de las personas.

---

[467] El término Industria 4.0, fue acuñado por el gobierno alemán para describir la fábrica inteligente, una visión de la fabricación informatizada con todos los procesos interconectados, a esto se denomina el Internet de las cosas. Mas Ingenieros está desarrollando soluciones industriales para el análisis de datos en el área del Big Data basadas en *open source*, aprovechando las ventajas de este tipo de plataformas y su indudable crecimiento en los últimos tiempos. Consultable en: http://www.masingenieros.com/portfolio/el-nuevo-reto-la-industria-4-0/

[468] En términos generales *Big Data*, podría entenderse como *la tendencia en el avance de la tecnología que ha abierto las puertas hacia un nuevo enfoque de entendimiento y toma de decisiones, la cual es utilizada para describir enormes cantidades de datos (estructurados, no estructurados y semi estructurados) que tomaría demasiado tiempo y sería muy costoso cargarlos a un base de datos relacional para su análisis. De tal manera que, el concepto de Big Data aplica para*

Las empresas, en los últimos años, poco a poco han ido añadiendo las comunicaciones y la tecnología de recolección de datos para sus procesos y ahora cuentan con los programas para analizar esa gran cantidad de datos. Esos programas permiten procesar enormes cantidades de datos, con independencia de la estructura o formato en el cual se conserven, por ejemplo, los datos producidos por dispositivos móviles, audio, video, sistemas GPS, incontables sensores digitales en equipos industriales, medidores eléctricos, veletas, anemómetros, cámaras, etc.

A modo de ejemplo, para ilustrar la captura masiva de datos por parte de las empresas, se tiene el reciente descubrimiento realizado por parte de la empresa Vizio (fabricante de televisores inteligentes en EE.UU. y número uno en ventas), al revelar la colección de datos de los usuarios. En apariencia, esta información fue revelada como parte del proceso llevado a cabo por esta compañía para vender parte de su capital en Wall Sreet. En los datos se muestra que colectan, en tiempo real, más de 100 billones de datos de forma diaria a través de más de 8 millones de unidades[469]. Estos datos son colectados con la intención de conocer los hábitos de consumo de los usuarios, a través de una tecnología capaz de rastrear el contenido y determinar lo que ven los usuarios en cada momento, con independencia de la fuente que proporciona las imágenes[470].

---

toda aquella información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales. BARRANCO FRAGOSOM, R., *¿Qué es Big Data?*, México, 2012, [en línea], http://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/index.html

[469] El detalle de la información, hasta ese momento oculta por parte de la compañía, puede ser consultada en: http://www.sec.gov/Archives/edgar/data/1648158/000119312515262817/d946612ds1.htm

[470] POZZI, S., "Cuando el televisor espía" en *El País,* 28 de julio de 2015, [en línea], http://economia.elpais.com/economia/2015/07/27/actualidad/1438001658_976873.html

La información generada por los usuarios de tecnologías es colectada por las compañías y produce alrededor de 2.5 quintillones de bytes[471] de forma diaria en el mundo. Solo Facebook almacena aproximadamente, 100 Petrabytes de fotos y videos[472].

Según el artículo citado, los programas de *Big Data* se alimentan, principalmente, de cinco tipos de información[473]:

1.- *Web and Social Media*: Incluye contenido web e información que es obtenida de las redes sociales como Facebook, Twitter, LinkedIn, etc., blogs.

2.- *Machine-to-Machine (M2M)*: M2M se refiere a las tecnologías que permiten conectarse a otros dispositivos. M2M utiliza dispositivos como sensores o

---

[471] A efectos de comparar, se muestra una escala de la cantidad de datos en cada uno de los términos utilizados:

Byte = 1

Kilobyte = 10^3 = 1000

Megabyte = 10^6 = 1,000,000

Gigabyte = 10^9 = 1,000,000,000

Terabyte = 10^{12} = 1,000,000,000,000

Petabyte = 10^{15} = 1,000,000,000,000,000

Exabyte = 10^{18} = 1,000,000,000,000,000,000

1 quintillón = 10^{30} = 1,000,000,000,000,000,000,000,000,000,000

El término byte fue acuñado por Werner Buchholz en 1957 durante las primeras fases de diseño del IBM 7030 Stretch. Originalmente fue definido en instrucciones de 4 bits, permitiendo desde uno hasta dieciséis bits en un byte (el diseño de producción redujo este hasta campos de 3 bits, permitiendo desde uno a ocho bits en un byte). Al efecto, puede consultarse en: https://es.wikipedia.org/wiki/Byte

[472] BARRANCO FRAGOSOM, R., *¿Qué es Big Data?*, *op. cit.,* [en línea], http://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/index.html

[473] *Ibíd.*

medidores que capturan algún evento en particular (velocidad, temperatura, presión, variables meteorológicas, variables químicas como la salinidad, etc.) los cuales transmiten a través de redes alámbricas, inalámbricas o híbridas a otras aplicaciones que traducen estos eventos en información significativa.

3.- *Big Transaction Data*: Incluye en la facturación de telecomunicaciones registros detallados de las llamadas (CDR), etc. Estos datos transaccionales están disponibles en formatos tanto semiestructurados como no estructurados.

4.- *Biometrics*: Información biométrica en la que se incluye huellas digitales, escaneo de la retina, reconocimiento facial, genética, etc. En el área de seguridad e inteligencia, los datos biométricos han sido información importante para las agencias de investigación.

5.- *Human Generated*: Las personas generamos diversas cantidades de datos como la información que guarda un *call center* al establecer una llamada telefónica, notas de voz, correos electrónicos, documentos electrónicos, estudios médicos, etc.

Si bien se considera que los programas *Big Data* se imponen de forma amenazante ante la intimidad de las personas, debe reconocerse las mejoras que producirán a futuro en todas las áreas del conocimiento humano.

Solo a efectos de ejemplificar una de ellas, se puede citar la aplicación de análisis de datos con *Big Data* realizada por la Universidad del Estado de Nueva York, en la investigación, el diagnóstico, tratamiento y una posible cura para la esclerosis múltiple[474].

---

[474] KOBIELUS, J., *Big Data analitics helps researchers drill deeper into multiple sclerosis,* 14 de mayo de 2012, [en línea], http://www.ibmbigdatahub.com/blog/big-data-analytics-helps-researchers-drill-deeper-multiple-sclerosis

Si bien *Big Data* se plantea en el terreno de la informática como el detonante de una cuarta revolución industrial, lo cierto es que, para su funcionamiento, se requiere de cantidades casi incalculables de información, entre la cual destacan datos de todas las categorías, incluidos los datos sensibles de las personas. El problema principal se produciría al asociar esos datos con una persona, pues se lesionaría el derecho de intimidad y la protección de los datos de carácter personal.

6.7. Delitos informáticos que protegen la intimidad.

Existen muchos riesgos en Internet que podrían afectar los derechos de las personas. En la mayoría de países[475] se han tipificado conductas relacionadas con los delitos informáticos[476] o ciberdelitos. Si bien estos delitos se traducen en delitos tradicionales como fraudes, estafas, espionaje, chantaje, falsificación, robo de identidad, entre otros, pero, también se han tipificado nuevas conductas no deseadas por la sociedad, incluidos nuevos delitos que afectan la intimidad.

Estas normas se han incluido en las legislaciones penales con el propósito de reprimir las conductas que se realizan por medios informáticos o telemáticos que atenten contra bienes jurídicos no patrimoniales o derechos fundamentales como el acceso a la información, la intimidad personal y familiar, el derecho de imagen, el honor, etc., o bien cuando atenten contra bienes patrimoniales genéricos o de tratamiento jurídico *sui géneris* como la propiedad intelectual e industrial.

---

[475] "*Las diferentes legislaciones del mundo han regulado este procedimiento informático desde el punto de vista del derecho administrativo y civil y para protegerlo como "ultimo ratio", en todo o en parte, se han añadido mecanismos jurídicos de tipo penal, para tutelar los derechos al acceso a la información, las facultades estructurales del habeas data (conocimiento, actualización, rectificación y cancelación de datos); y por supuesto, los derechos fundamentales, tales como la intimidad".* RIASCOS GÓMEZ, L. O., "El delito informático contra la intimidad de las personas: una visión constitucional y penal", *Ponencia presentada en el Congreso Latinoamericano de Derecho Informático,* Buenos Aires, 2004, [Biblioteca Vlex].

[476] Según advierte Miguel Ángel Davara, en la normativa no existe el *delito informático*, sin embargo, señala este autor que, se ha admitido llamar a las conductas antijurídicas realizadas a través de medios informáticos o telemáticos como *delitos informáticos,* los cuales albergan todos los delitos realizados a través de esos medios y los define como: "*la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software".* DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho Informático, op. cit.,* pp. 355-358. *V. et.* LEMAÎTRE PICADO, R., Manual sobre delitos informáticos para la ciber-sociedad costarricense, Investigaciones Jurídicas S.A, San José, 2011; CHINCHILLA SANDÍ, C., "Personalidad Virtual: Necesidad de una reforma constitucional" en *Revista de Derecho y Tecnologías de la Información,* N° 3-2005. UNED, San José, 2005, [en línea], http://www.egov.ufsc.br/portal/conteudo/personalidad-virtual-necesidad-de-una-reforma-constitucional; CHINCHILLA SANDÍ, C., *Delitos informáticos: elementos básicos para identificarlos y su aplicación en Costa Rica*, Farben Grupo Editorial Norma, San José, 2004.

Tal y como se había señalado, existen violaciones a la intimidad de forma física y electrónica (no físicas). Las primeras se refieren a las afectaciones a la intimidad por la intrusión de otra persona, sin embargo esta intrusión podría cometerse, también, por medios electrónicos, de forma no física, que representaría el segundo supuesto. De esta manera, los *delitos informáticos* que protegen la intimidad, fueron diseñados para proteger los agravios a la intimidad cometidos a través de medios informáticos o telemáticos, sin embargo, existe en la normativa penal delitos como la usurpación, delitos contra el honor, intervención de comunicaciones (análogas), violación de domicilio, y otros que podrían vulnerar el derecho de intimidad de las personas a través de otros medios no informáticos o telemáticos, aunque en el caso de las comunicaciones se contempla la posibilidad de que estas, también, pueden vulnerarse a través de medios electrónicos.

Entre los *delitos informáticos* que se han tipificado interesan los que protegen la intimidad de las personas, tales como: la revelación de secretos, la publicación de datos reservados, los accesos no autorizados, la interceptación de comunicaciones o datos personales, el apoderamiento de los secretos, la manipulación de datos reservados personales. El bien jurídico tutelado en los delitos señalados, tal y como apunta Blanco Lozano, no es otro que la intimidad[477].

El Derecho Penal se ha encargado de la tipificación de estas conductas como *ultima ratio* brindando protección al derecho de intimidad de las personas. Esta

[477] BLANCO LOZANO, C., *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*, Tratado de Derecho Penal Español, Tomo 2 – vol. 1, 2005, [Biblioteca Vlex].

protección surge a partir del registro de los datos de carácter personal, es decir, a partir de la fase informática que se llama de tratamiento o programación[478].

Los procesos informáticos contemplan cuatro fases principales, a saber: a) recolección y almacenamiento de datos; b) procesamiento de los datos; c) retroalimentación (feedback); y, d) transmisión de los resultados del proceso, ya sea en el mismo ordenador a ficheros destino, sea por medio de comunicaciones o acceso a periféricos en los ficheros que se depositan[479]. En cada una de estas fases podrían cometerse delitos.

Si bien la mayoría de delitos informáticos suponen una afectación a los datos informáticos (manipulación, acceso no autorizado, introducción de datos, o la utilización de datos para fines distintos), no todos producen, necesariamente, una afectación a la intimidad de la persona.

En el Título X Capítulo I del Código Penal Español[480], se incluyeron los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. De esta manera, en el apartado primero del artículo 197, se expone:

"1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de

---

[478] MORALES PRATS, F., "Protección penal de la intimidad, frente al uso ilícito de la informática en el código penal de 1995", en *Cuadernos de Derecho Judicial*, Escuela Judicial, Consejo General del Poder Judicial. C.G.P.J. No. XI, "Delitos contra la libertad y Seguridad", Madrid, 1996, pp. 146-196.

[479] *Cfr*. DAVARA RODRÍGUEZ, M. Á., Manual de Derecho Informático, *op. cit.,* p. 363.

[480] *Vid.* Código Penal Español, Título X, Capítulo I, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, [en línea], https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses."

En el tipo penal expuesto, se aprecia que de forma amplia protege la intimidad cuando se tiene acceso indebido a documentos, haciendo una referencia genérica a los mismos, entre los cuales se podrían inferir los documentos electrónicos o informáticos.

Una referencia precisa a estos últimos documentos se observa en el apartado 2 del artículo 197, al señalar:

"2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero."

Debe notarse que en este aparatado se hace referencia particular a los datos reservados de carácter personal o familiar contenidos en ficheros o soportes informáticos, electrónicos o telemáticos, ya sean públicos o privados castigándose las conductas de apoderamiento, utilización o modificación cuando no estén autorizadas por el titular de los datos.

Según Davara es indiferente para la protección si las comunicaciones entre las personas se realizan a viva vos o si se realizan mediante transferencia de datos informatizados[481].

El caso de que la información obtenida en los apartados citados 1 y 2 del artículo 197, sean revelados a otras personas o publicados, se prevé una agravante

[481] Cfr. DAVARA RODRÍGUEZ, M. Á., Manual de Derecho Informático, *op. cit.,* p. 379.

en la pena prevista (apartado 3, art. 197 Código Penal Español). Sin embargo, si un tercero que no ha participado en la obtención de los datos, pero enterado de la ilicitud de estos, los publica, la pena prevista es ligeramente inferior (par. 2° apartado 3, art. 197 Código Penal Español).

En caso de que las informaciones interceptadas contengan datos personales sensibles, es decir, datos que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior (apartado 5, art. 197 Código Penal Español).

Además, se contempla sanción para quien, sin autorización de la persona afectada, difunda, revele o ceda a terceros, imágenes o grabaciones audiovisuales que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona (apartado 7, art. 197 Código Penal Español).

De otra parte, en Costa Rica se han realizado una serie de reformas para introducir en la legislación penal los delitos informáticos y, tres de esas conductas contemplan el resguardo de la intimidad de las personas. El artículo 196 del Código Penal costarricense[482], indica que:

"Será reprimido con pena de prisión de tres a seis años 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."*

[482] *Vid.* Título IV, Delitos contra el ámbito de intimidad, Código Penal de Costa Rica, Ley No. 4573 de 15 de noviembre de 1970, [en línea], http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=98548&strTipM=TC

Este delito se refiere a la violación de correspondencia o comunicaciones y hace énfasis en que la conducta debe poner en peligro o causar un daño a otra persona en su intimidad o privacidad. En este artículo no se especifica si los documentos pueden ser electrónicos, sin embargo, en el artículo 196 bis del mismo texto legal se indica:

"Será sancionado con pena de prisión de tres a seis años 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."*

Se aprecia que el legislador ha incluido la protección penal de los datos personales en este último artículo, indicando expresamente que debe existir un peligro o daño para la intimidad o la privacidad de las personas. Además, se advierte que separa las imágenes de los datos e incluye la protección de intimidad de las personas jurídicas.

Otro de los delitos informáticos que protege la intimidad, introducido en la legislación penal costarricense, es el delito de suplantación de identidad, contemplado en artículo 230 del Código Penal, que indica:

"Será sancionado con pena de prisión de tres a seis años ***quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información****. La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero."*

Este delito en esencia protege la intimidad de las personas para evitar la suplantación de la identidad, otorgando un grado de protección especial a lo que se ha denominado en doctrina como *identidad virtual*[483].

La identidad de las personas, tal y como se ha señalado, es uno de los componentes importantes de la intimidad. Cada persona tiene derecho a determinar la información que desean compartir de forma pública y así "crear" o proyectar una imagen frente a los demás. Lo anterior sin dejar de lado los datos que sirven para identificar a las personas, los cuales suponen uno de los componentes de la imagen o identidad.

Se estima que *los derechos y libertades fundamentales* se ven amenazados como consecuencia de los avances tecnológicos, principalmente por el uso de Internet. Los derechos que se estiman más vulnerables, son los ejercitados a través de esta red, como la libertad de expresión, el acceso a la información, la vida privada de las personas, el secreto de las comunicaciones y la protección de los datos de carácter personal.

El desarrollo y el fortalecimiento de la seguridad informática es un asunto de actualidad. Existen varias causas generadoras de problemas que afectan la seguridad de los usuarios en Internet, ante lo cual se han implementado mecanismos desde diversas áreas de especialidad, para controlar o prevenir asuntos relacionados con la seguridad de los usuarios. Sin embargo, los que posean la mejor tecnología y más recursos, probablemente, serán capaces de concentrar la mayor cantidad de datos referidos a la intimidad de las personas y podrán constituirse como administradores de esa información.

---

[483] CHINCHILLA SANDÍ, C., "Personalidad Virtual: Necesidad de una reforma constitucional" en *Revista de Derecho y Tecnologías de la Información,* N° 3-2005. UNED, San José, 2005, [en línea], http://www.egov.ufsc.br/portal/conteudo/personalidad-virtual-necesidad-de-una-reforma-constitucional

Luego de la denuncia de Snowden sobre la vigilancia masiva por el gobierno de los EE.UU., particularmente por la NSA, la preocupación por la intimidad y privacidad se ha incrementado. La utilización de nuevos medios de almacenamiento en la nube ha experimentado un considerable crecimiento por parte de los usuarios, sustituyendo los medios tradicionales de almacenamiento de archivos electrónicos en sus propios equipos.

La popularidad de Internet y algunos servicios del web 2.0, como buscadores, redes sociales, webmail, entre otros, ha provocado que el tema de la privacidad de la información adquiera mayor trascendencia para la comunidad en general y no solo para los expertos del área de seguridad informática o las empresas.

Pese a esta preocupación y, más allá del extenso debate social y mediático que generó todo el tema de la NSA, las medidas de protección que adoptan los usuarios para resguardar la privacidad y seguridad de los entornos informáticos que utilizan (computadoras, teléfonos inteligentes, tabletas y otros) son, en muchas ocasiones, deficientes. Asimismo, producto de la falta de conciencia y exceso de confianza, las personas suelen actuar de un modo riesgoso con respecto a la seguridad de sus datos.

El derecho de intimidad y a la confidencialidad de los datos de las personas constituyen un derecho fundamental, necesario para que las personas sean respetadas como seres autónomos y libres, más aún si se considera que el cuerpo, la mente y los datos sociales y sanitarios forman parte de la intimidad, de la privacidad y de la confidencialidad de estas.

Se podría concluir que los derechos personales en general y, en particular aquellos que se ejercitan en Internet, resultan propensos a ser vulnerados por las nuevas tecnologías, dado su alcance y aparente falta de regulación. A ello se suman otros factores como la falta de educación, los intereses económicos, los intereses políticos y la capacidad de interconexión y convergencia.

Los expertos apuntan que Internet implica el riesgo de un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos y hacen una especial referencia a derechos como la intimidad, la imagen, la libertad sexual, la dignidad y el honor de las personas, así como a bienes e intereses jurídicos relacionados con la propiedad intelectual e industrial y la seguridad nacional y el orden público.

La sociedad actual se encuentra en una encrucijada con respecto a Internet, dado la eficacia global e ilimitada que tienen los hackers para atentar contra bienes y derechos desde cualquier parte del planeta, mientras que la capacidad de respuesta jurídica para defenderse se haya fraccionada por las fronteras nacionales. Por ello, la reglamentación jurídica del flujo interno e internacional de datos es uno de los principales retos que hoy se plantean los ordenamientos jurídicos nacionales y el orden jurídico internacional.

Por otro lado, el acceso a Internet ha sido todo un desafío en los países del tercer mundo y ha generado lo que se conoce como la “brecha digital”, la cual revela las diferencias en el acceso a Internet que pueden tener algunas personas, ya sea por su condición socio-económica, razones culturales o por residir en lugares en los cuales no se presta este servicio.

Internet está considerado como un derecho humano altamente protegido. Reconocimiento realizado por parte de la Asamblea General de la Organización de Naciones Unidas, la cual exigió a los países miembros que facilitaran servicio accesible y asequible para todos y estima como una prioridad asegurar a la ciudadanía el acceso a este servicio. Sin embargo, el uso de Internet, ha permitido que, con mucha facilidad, se puedan rastrear, almacenar, manipular, captar, cruzar, utilizar y transmitir piezas de información de las personas, o “*datos personales*”. Estas actividades pueden, en mayor o menor medida incidir de forma negativa en la intimidad, el secreto de las comunicaciones, el honor, la libertad sindical, la libertad religiosa o cualquier otro derecho fundamental, así como en otros derechos o intereses protegidos por el ordenamiento jurídico, dependiendo del uso, la finalidad y la intensidad con la que se realicen dichos actos.

Entre las múltiples amenazas a la intimidad, al secreto de las comunicaciones y a la protección de datos personales, se han identificado algunas prácticas o tecnologías que, debido a su naturaleza, hacen más propensas las violaciones de estos derechos fundamentales. En estas se encuentra la utilización de *cookies,* los proveedores del servicio de Internet ISP, la información biométrica, los motores de búsqueda, las redes sociales, el *cloud computing* y el *Big Data*.

Si bien las *cookies* son herramientas que tienen un papel esencial para la prestación de numerosos servicios de la sociedad de la información, que concentran la mayor inversión publicitaria, facilitan la navegación del usuario y ofrecen una publicidad basada en ocasiones en los hábitos de navegación, también son puntos débiles en lo que respecta a la privacidad de los usuarios. Por lo anterior, se han aplicado las normas relativas a la protección de datos personales, a la utilización de estos programas, en las ocasiones en que estos almacenen datos personales, como la Directiva 95/46/CE, la LODP y la LSSI.

Entre los datos almacenados por las empresas que prestan servicios relacionados con la TIC, se tienen los datos biométricos y las imágenes, datos que deben ser considerados como muy sensibles, al tratarse de datos que pueden identificar a las personas.

Algunos de estos datos, al proceder de rasgos físicos o biológicos de las personas y dado que permiten determinar su identidad y elaborar un perfil, tienen protección jurídica, razón por la cual no deben ser objeto de tratamiento externo no autorizado, puesto que tienen incidencia con el ámbito más íntimo y personal de las personas, cuyo tratamiento desautorizado puede incorporar peligro, no sólo de discriminación, sino que sean conocidos por terceras personas, a las que no queremos hacer partícipes de unos datos íntimos.

En la normativa europea los datos genéticos se encuentran protegidos de forma especial en el Convenio para la protección de los Derechos Humanos y la Dignidad del Ser Humano con respecto a las aplicaciones de la biología y la

medicina, también llamado Convenio relativo a los Derechos Humanos y la Biomedicina, elaborado por el Consejo de Europa, del 4 de abril de 1997 y la Declaración Universal sobre el Genoma Humano y los Derechos Humanos de la UNESCO, del 16 de noviembre del 1999.

De igual manera, los motores de búsqueda de Internet representan otro peligro con respecto al manejo de datos personales e intimidad de las personas. Dado que tienen la capacidad de almacenar la información de los usuarios para personalizar las búsquedas, acelerarlas y refinarlas en razón de los intereses de los usuarios.

De tiempo reciente, han cobrado importancia los buscadores que no almacenan información de los usuarios como DuckDuckGo, Starpage, Gibiru, Lukol, MetaGer (Alemania), Ecosia y Disconnect Search. Otros motores, como el de la empresa Seeks o Yacy, utilizan tecnologías peer to peer que, permiten realizar búsquedas en Google, Bing, Yahoo, Blekko de forma anónima.

La sentencia del Tribunal de Justicia Europeo con respecto a la empresa Google, en la cual se determinó la responsabilidad de los gestores de motores de búsqueda sobre el tratamiento de los datos de carácter personal que aparecen en las páginas web publicadas por terceros constituye probablemente una de las sentencias más importantes respecto a la protección de datos personales en los últimos tiempos.

Es necesario destacar los alcances de la nueva propuesta de Reglamento de Protección de Datos de la UE, en el cual se presenta la nueva posición jurídica de los ciudadanos frente a las grandes corporaciones internacionales que llevan a cabo tratamientos de datos personales a través de redes sociales virtuales, motores de búsqueda o servicios de computación en nube. Esta posición supone una considerable mejora al exigir de forma expresa el sometimiento a esta normativa de protección de datos, a las entidades no establecidas en la Unión Europea que traten datos de residentes en la Unión, para ofrecerles bienes o servicios o para controlar

su conducta (art. 3.3); además, los responsables del tratamiento de datos, no establecidos en la Unión, tienen que designar un representante en la misma (art. 25). Adicionalmente, los proveedores de servicios de Internet y las empresas que presten servicios de buscadores en línea, tienen la obligación de limitar la recogida de datos al mínimo necesario (art. 5.c), y deberán informar a los usuarios de forma transparente sobre quién recoge y usa sus datos y sobre cómo, con qué fines y por cuánto tiempo lo hace (arts. 14 y 15).

Desde la puesta en marcha de la Web 2.0, los perfiles sociales han causado una creciente preocupación para la privacidad en Internet. Este servicio ha facilitado el intercambio de información participativa y la colaboración a través de Internet en redes sociales.

En la actualidad se vislumbra una cuarta revolución, denominada la Revolución la “fábrica inteligente” o Industria 4.0, la cual se refiere al desarrollo del software, sistemas masivos de datos “Big Data” y su almacenamiento, la incorporación de sensores y electrónica a los elementos que interactúan en los procesos productivos y en los productos derivados de ellos, la convivencia hombre-máquina y la disponibilidad de la información enriquecida para una mejor y más acertada toma de decisiones.

La amenaza a la intimidad de las personas con la implementación de estos programas informáticos, radica particularmente en la posibilidad de analizar grandes cantidades de datos procedentes del entorno de las personas.

Algunas de las recomendaciones a los problemas expuestos para las empresas, podrían ser:

- Instruir a los usuarios sobre el tratamiento de datos personales, los medios publicitarios empleados en la plataforma, las situaciones de riesgo a las que se pueden enfrentar derivadas del uso de este tipo de servicios online, así como de las implicaciones que pueden derivarse de la publicación de contenidos en Internet.

- Explicar a los usuarios las medidas de seguridad que la plataforma ha implementado para actuar en caso de que se produzca la vulneración de alguno de sus derechos.
- Teniendo en cuenta que la gran mayoría de usuarios son menores de edad, resulta fundamental que las redes sociales y plataformas colaborativas, junto con las autoridades públicas, asociaciones y organizaciones, cuya finalidad sea la protección de este tipo de colectivos, lleven a cabo iniciativas conjuntas encaminadas a fomentar la formación entre los menores y tutores respecto a la seguridad de los usuarios, investigando las posibilidades tecnológicas existentes para lograr la identificación de la edad de los usuarios del servicio.
- Promover programas de voluntariado dentro de las empresas para colaborar con las instituciones escolares y centros de formación con el fin de difundir la importancia de la seguridad, así como para informar sobre las principales recomendaciones a tener en cuenta en el uso de este tipo de servicios.

Algunas recomendaciones para los usuarios de los servicios en Internet podrían ser:

- Considerar con detenimiento la publicación de datos personales (específicamente nombre, dirección o número de teléfono) en un servicio en línea. Plantearse si le gustaría encontrarse con información o imágenes en una situación laboral. Mantener la información de su perfil reservada.
- Usar un seudónimo en lugar del nombre real en los perfiles de Internet. Hay que tener en cuenta que incluso después tienen un limitado control sobre quién puede identificarlo, como terceras personas pueden ser capaces de levantar un seudónimo, especialmente basado en imágenes.

- Respetar la privacidad de los demás. Se debería tener especial cuidado con publicar información personal acerca de otros (incluyendo imágenes o fotografías), sin consentimiento de la otra persona.
- Informarse sobre qué empresa opera el servicio, bajo cuál jurisdicción, si existe un marco normativo adecuado para proteger la privacidad, si existe un mecanismo de supervisión independiente (como una Agencia de Protección de Datos) a la cual pueda acudir en caso de problemas, cuáles son las garantías que da el proveedor del servicio con respecto a la manipulación de sus datos personales, si el servicio ha sido certificado por entidades independientes y confiables, de buena calidad de privacidad y seguridad.
- Utilizar la web para educarse sobre la experiencia de otras personas con las mejores prácticas privacidad y seguridad. Utilizar el material existente de información de los proveedores de servicios de red social, pero también de fuentes independientes como Agencias de protección de datos y seguridad.
- Utilizar la configuración de privacidad de modo restringido. Restringir la disponibilidad de información tanto como sea posible, especialmente, con respecto a la indexación por los motores de búsqueda.
- Utilizar datos diferentes de identificación (usuario y contraseña) que aquellos que utiliza en otros sitios web.
- Utilizar oportunidades para controlar cómo un proveedor de servicios utiliza sus datos personales (perfil y tráfico).
- Prestar atención a la actividad de menores a su cargo en Internet, especialmente, en sitios web de redes sociales.

Como conclusión general, se estima, que existe un problema derivado de la falta de conciencia y exceso de confianza por parte de los usuarios con respecto al valor de sus datos personales, lo cuales podrían ser accedidos por cualquier persona. En muchos casos, los usuarios hacen públicos datos y características

personales en Internet, que en ningún caso expondrían en la vida cotidiana como ideología, orientación sexual y religiosa, etc.

Los datos personales pueden ser utilizados de forma lícita por terceros usuarios malintencionados. Hay que considerar que siempre existe la posibilidad de que traten, manipulen y publiquen información falsa o sin autorización del usuario, generando situaciones jurídicas perseguibles que pueden llegar a derivarse de este hecho.

CAPÍTULO V. NUEVAS DIMENSIONES DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL.

"We currently live in a world where extensive dossiers exist about each one of us. These dossiers are in digital format, stored in massive computer databases by a host of government agencies and private-sector companies. The problems caused by these developments are profound. But to understand the problems, we must first understand how they arose".[484]

[484] Actualmente vivimos en un mundo donde existen extensos expedientes sobre cada uno de nosotros. Estos expedientes se encuentran en formato digital, almacenados masivamente en bases de datos informáticas por una serie de agencias gubernamentales y empresas del sector privado. Los problemas causados por estos desarrollos son profundos. Pero para entender los problemas,

1. CONSIDERACIONES PRELIMINARES.

Para señalar la derivación del derecho a la protección de datos personales del derecho de intimidad, en el Capítulo III. 5 *supra*, se apuntaron los orígenes de este derecho, llegándose a la conclusión de que se trata de un derecho autónomo con respecto del derecho de intimidad, aunque estos derechos se encuentren imbricados y relacionados en aspectos esenciales.

La normativa que tutela este derecho[485], es uniforme al considerar como dato de carácter personal "*cualquier información concerniente a personas físicas identificadas o identificables*", lo que convierte en dato de carácter personal la mayor parte de la información sobre personas físicas, en la medida en que a través de escasos datos o informaciones sobre estas y mediante la correcta aplicación de herramientas informáticas, sería relativamente sencillo identificar a la persona concreta que se encuentra detrás de los datos que se dispone.

En EE.UU. los datos personales están protegidos de forma dispersa en la normativa. La interpretación de la Constitución realizada por la doctrina y sobre todo la jurisprudencia de la Corte Suprema, se ha ocupado de la protección de la privacidad. Diversos estatutos fueron creados como refuerzo, sobre todo luego de

---

primero debemos entender cómo surgieron [traducción libre del autor]. SOLOVE, D. J., *The digital person. Technology and privacy in the information age,* New York University Press, New York and London, 2004, [versión para lector digital Kindle].

[485] En España, se tiene el art. 2.a) de la Directiva 1995/46/CE; art. 3.a) de la Ley Orgánica 15/1999, de 13 de diciembre, sobre la Protección de Datos de Carácter Personal; art. 5.1 f) del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado mediante Real Decreto 1720/2007. En Costa Rica, se tiene el art. 3 inciso c) de la Ley de protección de la persona frente al tratamiento de sus datos personales.

los años setentas, a raíz de nuevas preocupaciones relacionadas con la creciente utilización de tecnologías[486].

Se estima que el marco legal en materia de protección de datos[487] responde a la necesidad de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, especialmente de su honor, intimidad y privacidad personal y familiar, evitándose así que los datos sean utilizados de forma inadecuada o fraudulenta, o sean tratados o cedidos a terceros sin consentimiento inequívoco del titular.

En la sociedad contemporánea destaca el avance tecnológico, el cual se nutre de los datos y registros de personas. No existe duda alguna de que la sociedad que conocemos hoy en día, es totalmente distinta a la que existía décadas atrás. A este nuevo modelo social se le ha llamado *sociedad de la información*[488], y su

---

[486] SOLOVE, D. J., *The digital person. Technology and privacy …, op. cit.,* [versión para lector digital Kindle].

[487] Una armonización legislativa internacional en los Estados Europeos sobre la protección de los datos personales sometidos a tratamiento informatizado por medios idóneos, constituía la aspiración capital del Convenio 108 del Consejo de Europa de 28 de enero de 1981. Esto es lo que se pretendió con el Convenio de Estrasburgo, y en efecto se logró. El Convenio Europeo de 1981, como también se le conoce, relativo a la protección de personas en relación con el tratamiento automatizado de datos de carácter personal, fue ratificado por España el 27 de enero de 1984, con lo cual a partir de allí perteneció a los Estados con leyes de protección de datos de la segunda generación. Este texto, constituye una norma jurídica de derecho interno en España, por el ingreso al ordenamiento jurídico (art.96.1 CE) y es un eficaz instrumento de interpretación de los derechos humanos, en lo referente al uso de la informática pues define aspectos básicos como el concepto de dato de carácter personal, fichero automatizado, tratamiento automatizado o la autoridad "controladora del fichero", que hoy se define como responsable.

[488] El término *sociedad de la información* fue acuñado en los años sesentas y está relacionado, usualmente, con las tecnologías informáticas y de telecomunicaciones. *Cfr.* CHIRINO SÁNCHEZ, A., *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica*, CONAMAJ, San José, 1997, p. 2.

principal característica es el vertiginoso avance de la tecnología, el cual ha modificado enormemente diversos ámbitos, entre ellos el jurídico.

Desde luego, si los ataques al derecho de intimidad son producto del desarrollo de nuevas tecnologías, lo lógico sería que los mecanismos tradicionales de protección existentes no fuesen adecuados para la protección y, en su lugar, debería considerarse una nueva dimensión. La tutela de los datos de las personas en una sociedad informatizada, debería adaptarse para el reconocimiento de ciertas facultades de control sobre el flujo de informaciones que circulan[489].

Las tecnologías de la sociedad de la información significan un reto permanente para los juristas, pues el constante flujo de información pone en riesgo la correcta utilización de los datos de las personas, situación que se ve agravada porque la normativa que regulaba la noción clásica del derecho a la intimidad resultaba, considerablemente, insuficiente. Señala Gozaíni[490] que, ante las transformaciones que sufre la sociedad en sus formas de comunicación y manejo de información, se hace necesario el desarrollo de nuevas formas de defensa y protección de datos, ante las eventuales agresiones que pudiera presentar para las personas este nuevo sistema[491].

---

[489] Para Davara Rodríguez "*la persona a lo largo de su vida, va dejando una enorme estela de datos que se encuentran dispersos y que, hoy en día, con la aplicación de los modernos medios tecnológicos, es posible agrupar y tratar en forma conjunta, interrelacionándolos y analizando significados e interpretaciones conexas, creando o estudiando a voluntad aquellos aspectos de un perfil determinado del individuo que sea de interés controlar o conocer*". DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho Informático, op. cit.,* p. 45.

[490] GOZAÍNI, O. A., *Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación,* Rubinzal-Culzoni Editores, Santa Fé, 2002, p. 9.

[491] En ese sentido apunta Campuzano que, *"la recopilación, utilización y libre circulación, cada vez mayor, de los datos personales exige por parte de los operadores del Derecho una atención particular. Máxime si se tiene en cuenta que las injerencias en la vida privada motivadas por la mala utilización del tratamiento de los datos informáticos, en la medida en que afectan al ámbito de la*

Estas tecnologías han permitido que el procesamiento de la información se realice a velocidades incalculables, así como se ha incrementado la capacidad de almacenamiento y transmisión de datos. La velocidad de este desarrollo de Internet y los servicios relacionados, en los últimos años, ha generado la creación de normativa para tratar de solventar los nuevos problemas suscitados, tratando de definir y desarrollar normas que garanticen la protección de los ciudadanos[492].

Pareciera que los esfuerzos de los legisladores se centraron, en un inicio, en las potenciales amenazas[493] de Internet como espacio de nuevas actividades delictivas, posteriormente de forma gradual, se realizaron esfuerzos para fiscalizar la actividad comercial electrónica, la protección de la propiedad intelectual y, de forma más reciente, la protección de la intimidad de los usuarios, incluyendo la protección de los datos personales y la discusión sobre temas como la neutralidad en Internet.

Tal y como se señaló en el apartado *supra* sobre la intimidad en Internet, los tipos de servicios, las *cookies,* los tipos de conexiones, los programas *Big Data* y, las redes sociales, se presentan como un riesgo potencial para los usuarios con respecto al tratamiento indebido de sus datos personales. Lo anterior además de

---

personalidad, producen efectos negativos irreparables. La violación del derecho a la vida privada no permite reparación posible; ¿qué sucedería si a través de las prácticas apuntadas se descubriera que alguien es seropositivo o que padece de una enfermedad genética incurable? Tales inmisiones en la vida privada de los sujetos producen consecuencias gravemente perjudiciales que deberían ser tomadas en consideración para otorgar la misma protección a los datos personales con independencia de cuál ha sido el ámbito, público o privado, en el que han sido recopilados y tratados". CAMPUZANO TOMÉ, H., *Vida privada y datos personales*, ed. Tecnos, Madrid, 2000, pp.65-66.

[492] *Ibíd*., p. 66.

[493] En el ámbito europeo este tema dio lugar a la aprobación del Libro Verde sobre *Protección de los menores y de la dignidad humana en los servicios audiovisuales y de información*, COM (96) 483 final; a la Comunicación de la Comisión sobre contenidos ilícitos y nocivos en Internet, COM (96) 487; y a la Resolución del Consejo de 28 de noviembre de 1996, sobre contenidos ilícitos y nocivos, *citado por,* CAMPUZANO TOMÉ, H., *op. cit.,* p. 66.

las posibles interceptaciones de datos o comunicaciones no autorizadas por parte de terceros, en perjuicio de la seguridad e intimidad de las personas.

La normativa relacionada con la protección de los datos personales, trata de resolver las situaciones planteadas como nuevos retos y nuevas amenazas, ofreciendo a las personas las garantías suficientes para tutelar su derecho a la vida privada. Desde luego, deben realizarse un reparto entre los derechos otorgados a los sujetos y las obligaciones para quienes procesen o ejerzan un control sobre los datos almacenados.

La relación existente entre intimidad y protección de datos personales obliga a tener en cuenta aquellos cambios que ha producido la incorporación masiva de la tecnología en la vida de las personas. La técnica de protección de datos pretende que todos estos sean dignos de tutela, para salvaguardar los aspectos de la vida privada de las personas y no sólo por desvelar aspectos íntimos o reservados.

Podría estimarse que la protección de los datos personales deja de tener una dependencia respecto al derecho a la intimidad, configurarse, el primero, como un derecho autónomo, de manera que permita a las personas la tutela sobre la circulación de la información que les interesa. Así, la protección de datos se convierte en un elemento central de la forma en la cual las personas viven y se relacionan en la sociedad de la información.

Para Miguel Ángel Davara la protección de datos se debe entender como *"…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, afecte a su entorno personal, social o profesional, en los límites de su intimidad"*[494].

[494] DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho Informático, op. cit.,* p. 49.

Del concepto anterior se pueden extraer tres características básicas que podrían delimitar el estudio de la protección de datos: a) que los datos sean susceptibles de tratamiento o se encuentren en soporte susceptible de tratamiento, b) la posibilidad de identificar el resultado del tratamiento de los datos con el titular y, c) que exista un manejo o acceso a los datos sin consentimiento del titular, independientemente de que este acceso o manejo se produzca en forma malintencionada o no.

2. DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES.

Los derechos fundamentales, incluidos los derechos personales, tienen su origen en la dignidad humana[495], según reconocimiento de las Constituciones modernas[496]. Esto constituye un punto de partida que deberá ser desarrollado en la práctica para que exista una verdadera protección de los derechos fundamentales.

En principio, la protección de datos se configura como un derecho autónomo y fundamental de las personas, que se concreta en la tutela -debido a la posible utilización de terceros no autorizados- de los datos personales susceptibles de tratamiento automatizado.

El derecho a la autodeterminación informativa adquirió rango de derecho fundamental cuando lo consagró como tal el Tribunal Constitucional Federal alemán, por primera vez, en la sentencia de 15 de diciembre de 1983, en la cual se pronunció sobre la Ley de 25 de marzo de 1982 referida al censo demográfico, la

---

[495] Según Luciano Parejo *"…la dignidad del hombre esté relacionada con la moralidad, con la superación de los instintos por el sentido de la moralidad a través del imperativo categórico. La dignidad humana es también, consecuentemente, una obra del propio hombre; no es otra cosa que una autoafirmación valorativa inducida por el respeto a la Ley moral. El hombre, desde su libertad (su libre arbitrio) pasa a ser, con ello, una conquista dinámica -progresiva y continuada-, es decir, histórica de la virtud y, a través de ella, de la dignidad"* PAREJO ALFONSO, L., "El derecho fundamental a la intimidad", *IUS ET PRAXIS*, Lima, Revista de la Universidad de Lima, No. 21-22, 1993, pp. 40-41.

[496] En la CE la dignidad humana está contemplada en el artículo 10.1, "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la Ley y a los derechos de los demás son fundamento del orden político y de la paz social".

que fue declarada inconstitucional debido al número de informaciones que solicitaba de los ciudadanos[497].

El derecho a la autodeterminación sobre los propios datos personales o libertad informática, consiste en la prerrogativa de la persona para disponer de la información que sobre sí misma exista en los registros o bases de datos, a fin de que esa información sea veraz, íntegra, actualizada, no intrusiva, y con las garantías de seguridad y de uso conforme a la finalidad para la que fue proporcionada.[498]

Afirmar que se trata de un nuevo derecho pareciera no ser pacífico en la doctrina. Lucas Murillo de la Cueva[499] estima que si no coinciden los ámbitos que se quieren defender con el derecho a la intimidad y la protección de datos personas, si aquél responde a una concepción preinformática, si esta va configurándose como un sector especializado del ordenamiento jurídico cada vez más articulado y denso, entonces tal vez convenga abandonar la referencia de la intimidad y encabezar la exposición de esta problemática con un epígrafe distinto. Como es evidente, no se trata únicamente de un cambio nominal, sino de una consideración sistemática.

La protección de datos de carácter personal es un derecho desarrollado, de forma general, en el ámbito comunitario[500] y en cada uno de los países de la

---

[497] *Vid.* ORTI VALLEJO, A., *Derecho a la intimidad e informática. Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada*, Editorial Comares, Granada, 1984, pp. 39-40.

[498] AVELEYRA, A. M., *El derecho de acceso a la información pública vs. El derecho de libertad informática* [en línea], http://profesor.sis.uia.mx/aveleyra/comunica/pdp.htm

[499] LUCAS MURILLO DE LA CUEVA, P. L., *El derecho a la autodeterminación informativa. La protección de datos personales frente al uso de la informática*, Editorial Tecnos, Madrid, 1990, p. 120.

[500] La Directiva 1995/46/CE puede ser considerada, a la fecha, la norma principal sobre la protección de datos personales.

Comunidad Europea. Por ejemplo, en España su regulación se lleva a cabo mediante Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y por Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD) y además existe un amplio desarrollo interpretativo por parte de la Agencia Española de Protección de Datos (AEPD)[501], que mediante sus resoluciones ha dado respuesta a casos de vulneración de derechos a la protección de datos, derivada del uso de los nuevos servicios que ofrece la Sociedad de la Información, lo que permite a los usuarios contar con la máxima garantía en la protección de sus derechos personales.

El derecho a la autodeterminación informativa tiene un contenido diferente al derecho a la intimidad[502], su ámbito es más amplio y los elementos que los componen resultan más complejos. Hay quienes consideran que este derecho se encuentra liberado respecto de la protección de la intimidad, de ahí que se configure como un derecho fundamental autónomo[503].

---

[501] AEPD: http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

[502] Una diferenciación clara y explicativa -la cual ya había sido expuesta- entre intimidad y Autodeterminación Informativa, puede inferirse de la consagración de ambos derechos en la Carta de los Derechos Fundamentales de la Unión Europea bajo la denominación de "…respeto de la vida privada y familiar" en su artículo 7. Esa norma hace alusión a la intimidad de manera concreta y, por otro lado, habla de manera independiente de la "…protección de datos de carácter personal" en el artículo 8. *Carta de los Derechos Fundamentales de la Unión Europea*. Art. 7 "…respeto de la vida privada y familiar" esa norma hace alusión a la intimidad de manera concreta y, por otro lado, el art. 8 indica, de manera independiente, sobre la "…protección de datos de carácter personal".

[503] El Tribunal Constitucional Español, en la STC 292/00 de 30 de noviembre, ha estimado dicha protección como un *nuevo derecho fundamental*, el derecho a la libertad informática, cuyo contenido básico es la protección de los datos sometidos a tratamiento informático y el reconocimiento al individuo de un poder de control sobre tales datos.

Si bien se puede estimar que la intimidad ha formado parte esencial en la construcción de la doctrina que sustenta el derecho a la protección de datos personales, lo cierto es que esta ya no puede seguir siendo concebida como una reserva de la esfera secreta e intangible de una persona frente a las demás, sino que, debería ser entendida como, el control de la información personal[504]. En ese sentido se habla de un cambio sustantivo, teniendo en consideración que en el derecho a la vida privada los mecanismos de tutela parten del supuesto que la persona tiene derecho a excluir interferencias ajenas sobre su vida, siendo la tutela en este caso estática y negativa. Sin embargo, en la protección de datos personales el argumento es distinto, pues su ejercicio se concreta en poderes de intervención, siendo la tutela dinámica, ya que protege los datos durante su recogida, tránsito y disposición.

En la jurisprudencia[505], la libertad informática o autodeterminación informativa se perfila como un nuevo derecho fundamental, con autonomía respecto al derecho de intimidad, el cual en lugar de entenderse como un derecho constitucional, se percibe como una garantía de la intimidad personal[506], entendida

---

[504] Miguel Castaño señala que *"(…) aun cuando la intimidad pudiera considerarse muy relacionada con el secreto, esta noción debe ser depurada, ya que no es cierto que cuanto menos se sepa de nosotros, gocemos de una mayor intimidad, ya que ésta no es simplemente la ausencia de información sobre cada uno en la mente de los demás, sino más bien el control que podemos ejercer sobre nuestra propia información personal"* MIGUEL CASTAÑO, A., "Libertad de información y derecho de intimidad: medios para garantizarla. Incidencia en el ámbito de la estadística", REDUC, número 12, septiembre de 1986, p. 175.

[505] *Vid.* STC 292/00 de 30 de noviembre.

[506] LÓPEZ GUERRA, L., *et. ál., op. cit.,* [versión para lector digital Kindle]. También, Mercedes Galán ha considerado que: *"…si la doctrina y la jurisprudencia plantean el nacimiento de un derecho nuevo, es precisamente para dar una respuesta a la incidencia de la informática sobre la intimidad. De ahí que no sea ya necesario el desdoblamiento de los derechos fundamentales que le sirven de sustento (la intimidad, el honor, la propia imagen, etc.) ni la ampliación de la protección inicialmente prevista por la Constitución para un derecho fundamental determinado. Una vez analizada la postura del Tribunal Constitucional y otras aportaciones doctrinales en relación con el derecho de la intimidad y el derecho a la autodeterminación informativa, nos adherimos a aquellas posiciones que consideran*

en un sentido amplio como la vida privada. En numerosas ocasiones se ha referido el Tribunal Constitucional al contenido y alcance de la libertad informática, y en esas oportunidades se ha considerado el significado especial de un derecho que se ha incorporado al elenco de bienes y derechos fundamentales[507].

Al efecto, el Tribunal Constitucional Español, ha estimado que el derecho de autodeterminación informativa o libertad informática está ligado estrechamente a la vida privada, como ámbito protegido en la constitución, pero no la necesita –derecho de intimidad-, para que se imponga como garantía frente a aquellos datos que sean relevantes en el ejercicio de los derechos de la persona, sean o no constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado.

"*De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o*

---

que la técnica de protección de datos no se centra ni mucho menos con exclusividad en lo que se viene entendiendo como intimidad", GALÁN JUÁREZ, M., *Intimidad. Nuevas dimensiones de un viejo derecho*, Editorial Universitaria Ramón Areces, Madrid, 2005, pp. 216 y 217.

[507] Una de las primeras resoluciones en la cual el Tribunal Constitucional Español se refiere al derecho de libertad informática es la STC 254/93 de 20 de julio.

no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado"[508].

Por lo anterior, podría estimarse el derecho a la protección de datos como una garantía constitucional independiente y autónoma del derecho de intimidad, la cual se impone ante al uso no autorizado de datos de personas cuando le puedan afectar otros derechos.

De la jurisprudencia del TCE podría inferirse que, ante a las nuevas tecnologías y la informática, la persona necesita una protección especial, con el propósito de amparar sus derechos fundamentales frente al uso ilícito o abusivo de esas tecnologías.[509]

Según la línea argumental contenida en la STC 254/93[510], se entiende que la intimidad informática o la libertad informática adquieren en la actualidad un matiz positivo, llegando a integrarse por un conjunto de facultades y de actuaciones positivas, las cuales permiten defender una nueva formulación y concepción jurídica del derecho a la intimidad personal y familiar, de forma que en la actualidad la intimidad asume un nuevo papel jurídico, en el cual se aleja de su concepción tradicional, para ser entendida como una nueva facultad y derecho individual, de naturaleza instrumental, como soporte de la protección y respeto de otros derechos también fundamentales.

---

[508] *Vid.* STC 292/00 de 30 de noviembre.

[509] *Vid.* STC 254/93, STC 143/94, STC 94/98, STC 144/99, STC 202/ 1999 y STC 292/2000.

[510] STC 254/93, la protección de datos personales se "... trata de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos".

La CE de 1978 incluye esta protección en el artículo 18.4[511] como mandato para el legislador, la cual había sido atendida en un inicio con la LORTAD[512], para ser reemplazada con la LODP[513] y su posterior desarrollo reglamentario.

En esta misma línea, la Carta de Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, incorpora y reconoce, según estándar europeo, el derecho a la protección de datos de carácter personal[514].

De otra parte, en Costa Rica, la CPC reconoce este derecho en el artículo 24. En la jurisprudencia de la Sala Constitucional costarricense se estima como un

[511] Art. 18.4 CE "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

[512] Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, conocida como LORTAD, tuvo como inspiración inmediata el Convenio 108 del Consejo de Europa, considerado como el primer texto que proclama principios y derechos sobre protección de datos personales, cuya referencia ha sido retomada por muchas de las legislaciones de los países miembros de la Comunidad.

[513] La Ley Orgánica de Protección de Datos de Carácter Personal de 13 de diciembre de 1999, conocida como LOPD, fue más bien una respuesta de adaptación de la normativa española del momento a las prescripciones europeas en la materia recogidas en la Directiva 95/46/CE sobre Protección de Personas Físicas en lo que respecta al Tratamiento de sus Datos Personales y a la Libre Circulación de estos, que recoge los principios del Convenio 108 pero amplia el contenido de la protección. Esta normativa se complementa con la Directiva Europea 97/66/CE del Consejo de 15 de diciembre de 1997 sobre el tratamiento de datos y la protección de la intimidad en las telecomunicaciones; y la Directiva 58/2002/CE del Consejo de 12 de julio de 2002 sobre datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas.

[514] Art. 8 de la Carta de Derechos Fundamentales de la Unión Europea: 1. "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen. 2. Esos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernen y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

verdadero derecho fundamental, es decir, le interpreta como un derecho autónomo con relación al derecho de intimidad[515].

Tanto en España como en Costa Rica este derecho se define como el poder de control de la persona sobre sus datos personales, sobre su uso y destino, como un poder de disposición permanente sobre todos los datos relacionados con la persona, que deben ser protegidos en su ejercicio, de forma que cualquier persona tenga capacidad de control sobre los mismos y conozca, en todo momento, quiénes tienen sus datos, con qué finalidades y pueda negarse a facilitarlos o bien modificarlos.

En Costa Rica no se contaba, hasta hace poco tiempo, con una ley especial de protección de datos, sin embargo, la tutela se ejercía de forma directa por medio de la Sala Constitucional, la cual creó basta jurisprudencia relacionada con la protección de datos personales. El 7 de julio de 2011 se aprobó la Ley No. 8968, Ley de protección de la persona frente al tratamiento de sus datos personales, por medio de la cual se creó la Agencia de Protección de Datos Personales (Prodhab), órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz, la cual tiene personalidad jurídica instrumental propia en el desempeño de las funciones que le asigna la ley, además de la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones, además, la Agencia goza de independencia de criterio[516].

En la Ley de protección de la persona frente al tratamiento externo e indebido de sus datos personales se distinguen cuatro categorías de datos personales, a efectos de determinar el grado de protección y acceso a esa información, esto son:

---

[515] *Vid.* SSC número 1999-04847 de las 16:27 hrs. del 22 de junio de 1999.

[516] Art. 15 de la Ley No. 8968, Ley de protección de la persona frente al tratamiento de sus datos personales.

los datos sensibles (máxima protección), los datos de acceso restringido (de protección media), lo datos de acceso irrestricto (sin protección) y los datos referentes al comportamiento crediticio (los cuales se rigen por las normas que regulan el Sistema Financiero Nacional).

Aunque en la Constitución de los EE.UU. no se utiliza la palabra *privacidad* (privacy) se protege esta al inferirse del texto, según se ha señalado por parte de la Corte Suprema de este país[517]. Al igual que en la mayoría de países que emplean el sistema de derecho continental, en este país también se ha extendido este derecho para dar protección frente al uso de nuevas tecnologías.

Como se ha indicado, en el derecho anglosajón, las políticas de privacidad por lo general son incluidas en los contratos, lo cual permite a las partes el reclamo por daños contractuales relacionados con violaciones a las políticas de privacidad. Desde 1998 la FTC es vista como la agencia federal de hecho para la protección de datos, adquiriendo esta potestad cuando el Congreso de los EE.UU. le atribuyó funciones particulares para la protección de datos a través de la Ley COPPA. El 31 de julio de 1998, el vicepresidente Al Gore anunció una serie de medidas dirigidas a la aprobación de una Carta de Derechos (Bill of Rights) electrónica, en particular medidas dirigidas a la reglamentación en materia de datos médicos y datos financieros, usurpación de la identidad y respeto de la vida privada de los niños, así como a favor de una autoregulación sectorial, entre otros campos, provista de mecanismos para asegurar esa protección.

Podría afirmase que la jurisprudencia del TEDH ha contribuido a la protección de estos derechos, lo cuales, con el trascurso del tiempo han ido evolucionando en la construcción europea sobre el derecho a la protección de datos personales,

[517] En el caso Whalen v. Roe en 1977, la Corte Suprema, extendió el debido proceso a la protección de la privacidad de la información. *Corte Suprema de los EE.UU.* caso Whalen v. Roe 429 U.S. 589 (1977).

protección que se ha hecho necesaria con la creación de tecnologías que posibilitan la racionalización, simplificación, celeridad y seguridad de las prácticas administrativas, públicas o privadas, incluyendo la recopilación de datos personales.

Podría concluirse que el tratamiento de los datos, en la mayoría de los países del sistema jurídico continental europeo, ha reconocido el derecho a la protección de datos personales como un verdadero derecho fundamental, en los países del *common law* se reconoce como un derecho constitucional, que además también se protege a través de normas estatutarias.

2.1. Concepto de autodeterminación informativa o libertad informática.

El derecho fundamental a la protección de datos personales contempla una serie de facultades y poderes de control para los titulares de la información, que en principio debería abarcar los procesos de elaboración y el uso de los datos, esto último relacionado con la acumulación, transmisión, modificación y cancelación. Ahora bien, estos datos personales han sido objeto de clasificación para facilitar el grado de protección que debería de otorgarse a través de la ley.

Esta facultad de control de los datos personales permite a los ciudadanos definir cuáles aspectos de la vida privada quieren compartir y cuáles poner en manos de otras personas, ya sean sujetos de derecho público o privado. Pareciera aceptado y uniforme en la doctrina que el derecho a la protección de datos personales es producto del avance de las tecnologías, las cuales permiten formas distintas del manejo de los datos, ubicando a las personas en posiciones vulnerables frente a la reserva de sus datos personales.

La doctrina sobre el tema de la protección de datos personales ofrece múltiples definiciones o conceptos. En ese sentido Delia M. Ferreira[518] señala que la autodeterminación informativa es "*la faceta más importante de la intimidad en el momento actual, y su defensa es el medio más eficaz para proteger la reserva de la vida privada en todas sus formas. Este derecho se manifiesta en dos direcciones: por un lado, en la posibilidad de mantener ocultos o reservados ciertos aspectos de la vida de una persona y por otro lado está la facultad de cada individuo de controlar el manejo y circulación de la información que, sobre su persona, esté en poder o haya sido confiada a un tercero."* Este concepto involucra la intimidad como punto

[518] FERRERIA RUBIO, D. M., *El derecho a la intimidad*, Editorial Universidad, Buenos Aires, 1982, pp. 14-17.

de partida para la protección de los datos personales, sin embargo, señala dos vertientes de forma expresa; la primera para la protección de aspectos de la vida privada de una persona y, la segunda, que se refiere a la facultad de disponer de la información de las personas.

En términos similares Rebollo Delgado entiende por "*intimidad informática*" el *"(…) contenido del derecho a la intimidad que establece la garantía de control y no injerencia sobre los datos relativos a la persona, susceptibles de tratamiento informático. Ello requiere el conocimiento por parte del individuo de la existencia y características de los bancos de datos que poseen datos a él relativos. De esta forma la extensión del derecho a la intimidad, en un ámbito concreto como la informática, lo que está haciendo es dar solución no a una nueva amenaza, sino a una forma o medio de llevarla a cabo"*[519]*.* El concepto ofrecido por el citado autor, fusiona la intimidad y la informática para referirse al derecho de protección de datos.

Una aclaración importante es que en este apartado no se propone como objetivo el debate doctrinal sobre el *nomen iuris* utilizado para conceptualizar el derecho de la protección de datos, por lo cual, se utilizarán como sinónimos los términos *libertad informática, intimidad informática, derecho de autodeterminación informativa o protección de datos personales*, sin mostrar ninguna preferencia de utilidad a efectos de la presente investigación.

Podría señalarse que el contenido esencial del derecho a la protección de datos en España y en la mayoría de los países de Europa y en varios de América, tiene dos ejes principales: por una parte, el consentimiento de la persona a quien los datos le conciernen y, por otra, el conjunto de derechos que lo hacen practicable -acceso, rectificación, cancelación y oposición- que garantizan el control de los

[519] REBOLLO DELGADO, L., *op. cit.*, p. 191.

datos y los principios de finalidad, pertinencia, utilización no abusiva, exactitud, lealtad, publicidad y de acceso individual.

Debe advertirse que el concepto de autodeterminación informativa o libertad informática ha sido equiparado o confundido con al concepto de intimidad o privacidad, pero como toda nueva redefinición, es una construcción moderna de un derecho antiguo, justificada en la utilización de tecnologías informáticas, pasando de un derecho negativo (a ser dejado a solas) a un derecho positivo, el cual permite, en principio, el control de la información de las personas. Así pareciera que se alude a discusiones doctrinales que fueron señaladas en el Capítulo II.2 *supra*, sin embargo, parece importante que se señale que se trata de derechos que se encuentran fuertemente amalgamados, sin perder la individualidad o fusionarse en otro distinto[520].

Podría afirmarse que toda información personal que puede afectar la dignidad o la libertad de las personas es susceptible de protección frente al poder informático, evitando con ello la intromisión en la vida privada de los individuos. Hoy día pareciera que no existen dudas sobre las tantas afectaciones que se configuran contra la intimidad de las personas, situación que ocasiona el desarrollo de la protección jurídica frente a estas conductas. Sin embargo, con el avance de las ciencias y la tecnología, nuevas amenazas seguirán surgiendo, las cuales pareciera provocarán el aumento en la tutela de estos derechos, en áreas como la protección de los datos genéticos, los pensamientos de las personas, el almacenamiento de las memorias de las personas y algunos otros más, como la introducción de

---

[520] *Cfr*. CARBALLO, E., "Informática y Protección de datos: Antecedentes para el proyecto de una ley nacional", *Revista del Colegio de Abogados de Buenos Aires*, núm. 3, 1986, p. 206; LYON, D., *El ojo electrónico. El auge de la sociedad de la vigilancia*, Alianza Editorial, Madrid, 1995, p. 32; y BEJAR, H., "Individualismo, privacidad e intimidad: precisiones y andaduras" en CASTILLA DEL PINO, C., *De la intimidad*, Crítica, Barcelona, 1989, p. 44.

información en las mentes de las personas, logrando modificar los pensamientos y acciones de las personas[521].

De otra parte, en la doctrina estadounidense, varios autores[522] estimaron que el derecho a la privacidad está determinado por el poder de control sobre la información personal. Estiman que la privacidad no es, solamente, la ausencia de información sobre la persona, sino también que se refiere al control que la persona ejerce sobre la información de sí misma que los demás pueden disponer. De esta manera, la privacidad, por tanto, es la facultad de control sobre los datos personales de uno mismo que los demás puedan acceder, y no sólo es un control de carácter cuantitativo, de la cantidad de información personal a disposición de los demás, es también un control cualitativo, del tipo de información que pueda disponerse, aunque el contexto social imperante determinará sobre qué clase de información personal se tendrá mayor control. Pareciera que, en definitiva, para el citado autor, el derecho a la privacidad no es la ausencia de información personal, sino que se refiere a la sensación de seguridad en el control sobre tal información.

Probablemente, uno de los autores más connotados de en el ámbito legal estadounidense, relacionado con el derecho de privacidad, es Alan Westin[523], quien estimó que la privacidad se refiere al control de la información personal, en

---

[521] *The talking window*. Una nueva plataforma de anuncios fue revelada por las compañías BBDO alemana y la emisora Sky holandesa. Según la noticia, estas empresas son capaces de introducir anuncios en los cerebros de las personas mientras recuestan sus cabezas en las ventanas del metro. KNOWLES, D., "German company tests 'talking window' that pumps ads into brains of train passengers" en *New York Daily News*, 5 de julio de 2015, [en línea], http://www.nydailynews.com/news/world/talking-window-advertising-technique-tested-germany-article-1.1391390

[522] FRIED, C., "Privacy", en *Yale Law Journal*, vol. 77, 1967-1968, pp. 475-493; MILLER, A., "The Assault on Privacy: Computers, Data Banks and Dossiers", *Ann Arbor, University of Michigan Press*, 1971, p. 25; GROSS, H., "The Concept of Privacy", en *New York University Law Review*, vol. 42, 1967, pp. 35-36.

[523] WESTIN, A., *Privacy and Freedom*, *op. cit.*, p. 7 y ss.

particular, como el derecho a decidir cuándo, cómo y en qué medida la información personal es comunicada a otros, como un mecanismo de autodeterminación personal que ha de integrarse en los procesos comunicativos y participativos en los que interviene el individuo. Por lo anterior, la pretensión del individuo de mantener privacidad no es absoluta, dado que su deseo de participar en la sociedad es, igualmente, poderoso, muy atractivo y muchas veces necesario. De esta manera, cada persona está, de forma continua y constante, involucrada en un proceso de adaptación personal, mediante la cual expresa su voluntad de privacidad con la de relación y comunicación con los demás, en función del contexto social. Westin afirmaba que la privacidad es un elemento necesario para la toma de decisiones y para la misma definición de la autonomía individual, de ahí que la privacidad sea un lubricante vital para el sistema organizativo de toda sociedad libre.

En la doctrina contemporánea de los EE.UU., Paul M. Schwartz[524] estima la conceptualización de la privacidad como un derecho de control sobre la información personal, supone el reconocimiento y la existencia de un importante ámbito de autonomía individual. Sin embargo, esta concepción no le parece satisfactoria, no sólo porque conlleva una visión mercantilista de la privacidad, cercana al derecho de propiedad intelectual, sino también porque en el ámbito de las tecnologías de la información y comunicación, y especialmente en Internet, se registran importantes limitaciones para el control real de la información personal, principalmente por la complejidad técnica del medio y por la ausencia de información clara y disponible para los usuarios sobre políticas de privacidad.

[524] SCHWARTZ, P. M., “Privacy and Democracy in Cyberspace”, en *Vanderbilt Law Review*, vol. 52, 1999, pp. 1609-1701; SCHWARTZ, P. M., “Internet, Privacy and the State”, en *Connecticut Law Review*, vol. 32, 2000, pp. 815-859.

2.2. Nuevos conceptos y retos en materia de protección de datos personales e intimidad.

2.2.1. La intimidad cognitiva.

Se propone este concepto de *intimidad cognitiva* para denominar la posible protección de los datos contenidos en los cerebros de las personas y que exista la posibilidad de extraerlos o implantarlos, tales como sus pensamientos, imágenes, recuerdos, conocimientos, etc. Ciertamente, se reconoce que aún no existen dispositivos con tales capacidades, sin embargo, recientes experimentaciones han traído a la mesa de estudio el hecho de plantear alguna protección legal para el momento en que esto pueda suceder.

En la actualidad, tal y como se indicó, no existe ninguna tecnología conocida para escuchar los pensamientos de las personas. Pero los avances de las imágenes por resonancia magnética funcional han demostrado que existen formas de mapear las ondas cerebrales. Entonces ¿será este el momento en que se tenga que proteger la privacidad cognitiva? Desde el año 2013[525] investigadores de la Universidad de Texas, en conjunto con la empresa coreana Samsung están trabajando en dispositivos (tecnología de neuro-monitores) de control mental para tabletas, lo cual en poco tiempo se convertirá en un nuevo *gadget o wearable*[526] del mundo de las computadoras.

---

[525] LIMER, R., "Samsung Is Working on Mind-Control for Its Tablets" en *Gizmodo,* 20 de abril de 2013, [en línea], http://gizmodo.com/5995131/samsung-is-working-on-a-mind-controlled-tablet-interface

[526] *Werable Computing* (vestimentas computadorizadas). Se refiere a los objetos y ropa de uso diario, tales como relojes y gafas, en las cuales se incluyeron sensores para extender sus funcionalidades. Las vestimentas son susceptibles de ser adoptados rápidamente, medida que se extiende a la utilidad de los objetos cotidianos que son familiares para el individuo, tanto más ya que apenas

¿Se convertirán estas tecnologías en una nueva forma de minería de datos? Probablemente, al llegar esas tecnologías, se piense en la regulación de los datos obtenidos de las mentes de las personas, cuestiones éticas, religiosas y de salud serán claves para determinar una posible regulación del uso de estos dispositivos y los límites que podrán imponerse a los fabricantes y desarrolladores.

¿Quién quiere vivir para siempre? Este es el eslogan publicitario de la empresa Eternime, Inc[527]. la cual ofrece un servicio en línea para guardar las memorias de las personas fallecidas. Se trata de un servicio que está en proceso de construcción, cuya meta es crear un legado interactivo transferido a un avatar de inteligencia artificial que emularía la apariencia y personalidad de las personas que han fallecido para que familiares y amigos puedan interactuar y no olvidarle[528]. Randal A. Koene es el Director de Ciencias del proyecto denominado Iniciativa 2045, que pretende como meta hacer una copia del cerebro humano completo, pero con capacidades funcionales[529].

De otra parte, Kevin Warwick, quien trabaja para la Universidad Europea de Madrid, ha creado implantes cibernéticos, principalmente destinados a la

---

pueden diferenciarse de sus prendas no conectadas. Pueden integrar cámaras, micrófonos y sensores que graban y transfieren datos al fabricante del dispositivo. Además, la disponibilidad de sensores para dispositivos portátiles también apoya la creación de aplicaciones de terceros, que pueden obtener de este modo el acceso a los datos recogidos por esas cosas. WP29 Opinión 8/2014, sobre la reciente evolución del Internet de las cosas, de 16 de setiembre de 2014, [en línea], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[527] El servicio de la empresa se encuentra en proceso de construcción y puede ser consultado en: http://eterni.me/

[528] *Vid*. PARKIN, S., "Back-up brains: The era of digital immortality", en *BBC Future*, 23 de enero de 2015, [en línea], http://www.bbc.com/future/story/20150122-the-secret-to-immortality

[529] *Vid. http://www.randalkoene.com/*

localización de personas. Sin embargo, estima que estos dispositivos, a futuro, podrán enviar mensajes telepáticos o grabar experiencias de la mente y tener acceso a los recuerdos[530].

Así mismo, ya se ha registrado la primera transmisión cerebral a través de Internet, en la cual un equipo internacional de neurocientíficos y robótica ha logrado la primera comunicación directa de cerebro a cerebro con seres humanos a través de una tecnología no invasiva[531].

El Grupo de Neuroingeniería Biomédica de la Universidad Miguel Hernández de Elche (Alicante) ha desarrollado una interfaz cerebro-computador que permite a un usuario navegar por Internet y manejar aplicaciones informáticas utilizando sólo el pensamiento, que la interfaz usa señales electroencefalográficas (EEG) que son recogidas mediante más de medio centenar de electrodos superficiales colocados sobre la cabeza del sujeto[532].

Las citadas noticias y artículos sobre al avance de las tecnologías que permiten el acceso a los recuerdos, memorias y pensamientos, se muestran como un ejemplo del tipo de datos que serán almacenados a futuro, lo cual, sin duda creará un replanteamiento de los sistemas y mecanismos que se utilizan actualmente para proteger, en un futuro cercano, los datos obtenidos de los

---

[530] DÍAZ, Á., "Kevin Warwick, el fabricante de microchips para localizar a niños secuestrados", en *elmundo.es,* 20 de noviembre de 2007, [en línea], http://www.elmundo.es/elmundo/2007/11/18/ciencia/1195408188.html

[531] GRAU, C., *ét. al.,* "Conscious Brain-to-Brain Communication in Humans Using Non-Invasive Technologies", en *PLOS one,* 19 de agosto de 2014, [en línea], http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0105225

[532] SANZ, E., "Navegando por Internet con el pensamiento" en *muyinteresante.es,* [en línea], http://www.muyinteresante.es/tecnologia/articulo/navegando-por-internet-con-el-pensamiento

cerebros de los seres humanos. Es probable que no exista otra una forma más directa de exponer a la intimidad de una persona que accediendo a sus recuerdos y pensamientos.

2.2.2. La privacidad en el diseño o privacidad desde el diseño (PdD).

Desde 1995 Ann Cavoukian[533] desarrolló este concepto *privacy by desing* (PdD) 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. La intención se basa en que la privacidad no puede estar asegurada, únicamente, por los marcos regulatorios, este aseguramiento debe convertirse en el modo de operación predeterminado de una organización.

En su acepción más clásica, la PdD se extiende a tres aplicaciones que la engloban: 1) sistemas de tecnologías de la información; 2) prácticas de negocio responsables; y 3) diseño físico e infraestructura en red[534].

Según Pablo García, la PdD se basa en una noción sustantiva de privacidad, que opera como un método para proteger la privacidad en su vertiente sustantiva, mediante lo que se puede entender como una "imprimación" de la privacidad en el corazón de los sistemas y procesos[535].

---

[533] CAVOUKIAN, A., "Privacy by Design, Curriculum 2.0", en *Information and Privacy Commissioner of Ontario*, [en línea], https://www.privacybydesign.ca/index.php/publications/curriculum/

[534] *Ibíd.*

[535] GARCÍA MEXÍA, P., *Derechos y libertades, internet y tics, op. cit.,* p. 26.

Para Miguel Ángel Davara[536], la PdD se presenta como la obligación de los desarrolladores y creadores de aplicaciones informáticas de introducir los principios básicos de la privacidad en el propio diseño de las aplicaciones de forma que, desde las primeras y más básicas especificaciones hasta el desarrollo propiamente dicho, pasando por los análisis y planteamientos elementales de cara a la solución del problema, se vean cumplidos estos principios. Para el citado autor, un ejemplo claro puede observarse en el principio de calidad de los datos o, expresado de otra forma, de minimización de los datos a tratar, tanto en el diseño como en el tratamiento, de manera que estos sean adecuados, pertinentes y no excesivos, de acuerdo con la finalidad y limitados al mínimo necesario, en relación a los fines para los que se traten.

Se atribuye a la PdD la posibilidad de atender un problema como lo es la falta de estándares internacionales que permitan homogenizar un concepto legal. En este sentido, el 16 de octubre de 2010 se hizo público el Dictamen del Supervisor Europeo de Protección de Datos[537] acerca de la promoción de la confianza en la sociedad de la información, mediante el impulso de la protección de datos y la privacidad, en el cual se debate la necesidad de integrar a nivel práctico la protección de datos y la privacidad, desde el inicio mismo de las nuevas tecnologías

---

[536] DAVARA RODRÍGUEZ, M. Á., "El tratamiento de datos de carácter personal y la utilización de la tecnología: entre la ética y el derecho" en *Diario La Ley*, Nº 8157, 26 de Setiembre, 2013, [en línea], http://www.juntadeandalucia.es/institutodeadministracionpublica/aplicaciones/boletin/publico/boletin56/Articulos_56/Davara-Rodr%C3%ADguez.pdf

[537] Dictamen del Supervisor Europeo de Protección de Datos de 16 de octubre de 2010, No. 2010/C 280/01, Bruselas, [en línea], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:280:0001:0015:ES:PDF, en adelante se nombrará (Dictamen No. 2010/C 280/01).

de la información y la comunicación, lo que se denomina el “principio de privacidad desde el diseño”.

En este se estima que, para imponer el cumplimiento de este principio, es necesario adaptar el marco jurídico de protección de datos, al menos de dos modos diferentes: en primer lugar, integrando el principio de “privacidad desde el diseño” como un principio general y vinculante y, en segundo lugar, incorporándolo en determinados ámbitos de las TIC que presentan riesgos concretos relacionados con la protección de los datos y la privacidad, mitigables mediante una arquitectura técnica y un diseño adecuados[538].

El Dictamen presta especial atención a la identificación por radiofrecuencia (RFID)[539], las aplicaciones de redes sociales y las aplicaciones de navegación. Junto a esto, el Dictamen formula una serie de sugerencias relativas a otras herramientas y principios orientados a proteger la privacidad y los datos de las personas en el sector de las TIC[540].

En el citado dictamen, se exponen las ventajas de esta solución para diseñar y desarrollar las TIC de modo que respeten la privacidad y la protección de los datos. Lo anterior por cuanto resulta crucial que la privacidad y la protección de los datos

---

[538] Dictamen No. 2010/C 280/01, párrafo 6.

[539] RFID (siglas de Radio *Frequency Identification*) significa identificación por radiofrecuencia. Los principales componentes de la tecnología de identificación por radiofrecuencia son una etiqueta (es decir, un microchip), un lector y una aplicación que está vinculada a las etiquetas y los lectores mediante middleware y que trata los datos producidos. La etiqueta consiste en un circuito electrónico que almacena los datos y una antena que los comunica por ondas de radio. El lector consta de una antena y un demodulador que traduce la información analógica recogida en forma de datos digitales. A continuación, la información se puede enviar por medio de redes a bases de datos y servidores, para ser procesada por un ordenador. Dictamen No. 2010/C 280/01.

[540] *Ibíd.*

se integren en todo el ciclo de vida de la tecnología, desde la primera fase del diseño hasta su uso y su eliminación[541].

Es claro que la PdD puede suponer diferentes acciones, dependiendo del caso o la aplicación concretos. Por ejemplo, en algunos casos puede obligar a eliminar o reducir datos personales o evitar tratamientos innecesarios o no deseados. En otros casos, la PdD puede dar lugar a que se ofrezcan herramientas para aumentar el control que tienen las personas sobre sus datos personales. Estas medidas se deberían tener en cuenta al definir los estándares o las mejores prácticas. También se podrían incorporar en la arquitectura de los sistemas de información y comunicación, o en la organización estructural de las entidades que tratan datos personales[542].

Existen siete principios básicos de la PdD, los cuales fueron expuestos por Cavoukian[543] de la siguiente manera:

1. Proactivo, no Reactivo; Preventivo no Correctivo. El enfoque de PdD está caracterizado por medidas proactivas, en lugar de reactivas. Anticipa y previene eventos de invasión de privacidad antes de que estos ocurran. La PdD no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron, su finalidad es prevenir que ocurran. En resumen, PdD llega antes del suceso, no después.

2. Privacidad como la Configuración Predeterminada. La PdD busca entregar el máximo grado de privacidad asegurándose de que los datos personales estén protegidos automáticamente en cualquier sistema de IT dado o en cualquier

---

[541] Dictamen No. 2010/C 280/01, párrafo 19.

[542] Dictamen No. 2010/C 280/01, párrafo 20.

[543] CAVOUKIAN, A., “Privacy by Design Curriculum 2.0”, *op. cit.,* [en línea].

práctica de negocios. La persona no toma una acción, aun así, la privacidad se mantiene intacta. No se requiere acción alguna de parte de la persona para proteger la privacidad está interconstruida en el sistema, como una configuración predeterminada.

3. Privacidad Incrustada en el Diseño. La PdD está incrustada en el diseño y la arquitectura de los sistemas de Tecnologías de Información y en las prácticas de negocios. No es un suplemento, después del suceso. El resultado es que la privacidad se convierte en un componente esencial de la funcionalidad central que está siendo entregada. La privacidad es parte integral del sistema, sin disminuir su funcionalidad.

4. Funcionalidad Total. La PdD busca acomodar todos los intereses y objetivos legítimos de una forma "ganar-ganar", no a través de un método anticuado de "si alguien gana, otro pierde", donde se realizan concesiones innecesarias. La PdD evita la hipocresía de las falsas dualidades, tales como privacidad versus seguridad, demostrando que sí es posible tener ambas al mismo tiempo.

5. Seguridad Extremo-a-Extremo. Habiendo sido incrustada en el sistema antes de que el primer elemento de información haya sido recolectado, la PdD se extiende con seguridad a través del ciclo de vida completo de los datos involucrados. Las medidas de seguridad robustas son esenciales para la privacidad, de inicio a fin. Esto garantiza que todos los datos son retenidos y luego destruidos con seguridad al final del proceso, sin demoras. Por lo tanto, la PdD garantiza una administración segura del ciclo de vida de la información, desde la cuna hasta la tumba, desde un extremo hacia el otro.

6. Visibilidad y Transparencia. La PdD busca asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada, deben operar de acuerdo a las promesas y objetivos declarados, sujeta a verificación independiente. Sus partes componentes y operaciones permanecen visibles y transparentes, a usuarios y a proveedores.

7. Respeto por la Privacidad de los Usuarios. Por encima de todo, la PdD requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas, que ofrezcan medidas tales como predefinir modos de privacidad robusta, notificación apropiada, y facultar opciones amigables para el usuario.

Según explica Davara[544], la noción de PdD está ligado al concepto de Privacidad por Defecto (PpD) y en muchas ocasiones se tratan como sinónimos, cuando lo correcto es diferenciarlos. Estos conceptos se complementan y presentan una estructura lógica operativa única para proteger la privacidad, en el primer caso se protege desde el origen, mientras que en segundo se protege el tratamiento.

La propuesta para el Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) del 27 de enero de 2012[545], plantea en el artículo 23 la protección de los datos desde el diseño y por defecto[546]. El objetivo principal de este Reglamento general es elevar el nivel de la protección de datos de las personas físicas y mejorar las oportunidades para las empresas en el mercado único digital.

En principio, esta propuesta de Reglamento general mejorará los niveles de protección de los datos personales, para que sean recopilados y tratados

---

[544] DAVARA RODRÍGUEZ, M. Á., "El tratamiento de datos de carácter personal y la utilización de la tecnología: entre la ética y el derecho", *op. cit.,* [en línea].

[545] Propuesta del Reglamento General de Protección de Datos de la U.E., [en línea], http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=es

[546] El 15 de junio de 2015, los Ministros de Justicia y Asuntos de Interior alcanzaron "una orientación general" sobre dicho Reglamento. Basándose en este acuerdo, el Consejo ya puede iniciar las negociaciones con el Parlamento Europeo (diálogos tripartitos). "Una orientación general" significa que el Consejo llega a un acuerdo político sobre cuya base puede ya iniciar las negociaciones con el Parlamento Europeo con el fin de aprobar nuevas normas de protección de datos en la UE.

lícitamente, en condiciones estrictas y con un fin legítimo. Los responsables del tratamiento (que responden del tratamiento de los datos) deben respetar unas normas específicas, como la exigencia del consentimiento inequívoco del interesado (la persona cuyos datos personales son tratados), para que se le permita tratar los datos personales.

Además, se refuerzan los derechos a la protección de datos, lo que permite a los interesados un control mayor de sus datos personales:

- Acceso más fácil a sus datos.
- Información más detallada sobre lo que ocurre con sus datos personales una vez decidan compartirlos: los responsables del tratamiento deberían ser más transparentes en cuanto al modo en que se manejan los datos personales, por ejemplo, informando a las personas físicas sobre su política de intimidad, con un lenguaje claro y sencillo.
- Se refuerza el derecho a la supresión de los datos personales y el "derecho al olvido", que permite a cualquiera exigir, por ejemplo, a un proveedor de servicios que suprima inmediatamente los datos personales recopilados durante la infancia de la persona.
- Se incluye el derecho a la portabilidad, que facilita la transmisión de datos personales de un proveedor de servicios a otro, como por ejemplo un cambio de una red social a otra. Ello incrementará también la competencia entre proveedores de servicios.
- Y finalmente, se establecen límites a la elaboración de perfiles, es decir, al tratamiento automatizado de datos personales para evaluar aspectos personales como el rendimiento en el trabajo, la situación económica, la salud, las preferencias personales, etc.

Pareciera razonable que se piense que la normativa relacionada con la protección de datos, en particular la Directiva 95/46/CE, luego de varios años de estimarse la norma principal frente a la protección de datos personales, deba

replantearse una nueva reglamentación como la propuesta, pues ello responde a nuevas necesidades de protección, como consecuencia del avance y de nuevos escenarios planteados por el desarrollo, siempre creciente, de las tecnologías de información y comunicación.

2.2.3. La privacidad por defecto (PpD).

La privacidad por defecto (PpD), y la PdD, podrían reconocerse como instrumentalizaciones de la protección de los datos personales, las cuales son necesarias dadas las limitaciones propias de la regulación legal en esta materia. Ciertamente, estas medidas colaboran en la protección de los datos personales, y aseguran algunas cuestiones elementales en los procesos que manejan datos de las personales.

La PpD simplemente significa que la configuración de privacidad más estricta se encuentra dispuesta de forma automática una vez que un cliente adquiere un producto o servicio. Además, aplica a un elemento temporal relacionado con el tiempo en que se almacenará esa información, el cual deberá ser el necesario para proporcionar el producto o servicio.

La descripción anterior se incorpora, tal y como se indicó en el apartado anterior Cap. V.2.2.2 *supra*, al art. 23 de la propuesta de Reglamento general de protección de datos del 27 de enero de 2012[547]. Ahora bien, existen posiciones encontradas en relación a la implementación de estas medidas, al estimar que no son ajustables a las aplicaciones móviles, que en su lugar debería de regular la

[547] Propuesta del Reglamento General de Protección de Datos de la U.E., [en línea], http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=es

cantidad de *privacidad* que requieren para el funcionamiento y el servicio demandado[548].

Esta medidas de PdD y PpD también ha sido sugeridas por el Grupo de Trabajo del Artículo 29 sobre protección de datos (WP29)[549], el cual ha rendido varios dictámenes en los que se sugiere la integración de estas medidas, como por ejemplo en el Dictamen 8/2014 relacionado al recientes desarrollo del Internet de las Cosas o *Internet of Things* (IoT)[550].

Sin duda podría afirmarse que el IoT plantea una serie de desafíos importantes para la privacidad y la protección de datos, algunos nuevos, otros más tradicionales, amplificados con respecto al aumento de la capacidad en el procesamiento de datos. De ahí surge la necesidad de considerar modificaciones a las normativas locales e internacionales relacionas con la protección de datos y la privacidad.

---

[548] *Vid.* Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Varsovia (Polonia), del 23 al 26 de septiembre de 2013, en la cual se tomaron varias resoluciones relacionadas con la protección de la privacidad y los datos personales, [en línea], https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/news/2013_10_01_3-ides-idphp.php

[549] El Grupo de Trabajo se creó en 1996 (en virtud del artículo 29 de la Directiva 95/46/CE) con carácter consultivo y estaba compuesto por representantes de las autoridades nacionales de control de la protección de datos (ACPD), el Supervisor Europeo de Protección de Datos (SEPD) y la Comisión. Para más información sobre sus actividades, véase http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

[550] WP29, Dictamen 8/2014, sobre la reciente evolución del Internet de las cosas, de 16 de setiembre de 2014, [en línea], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

2.2.4. Internet de las cosas (IoT).

Según el FTC Staff Report de IoT, de enero de 2015[551], la tecnología rápidamente, está cambiando la forma de interactuar con el mundo que nos rodea. Hoy en día, las empresas desarrollan productos para el mercado de consumo que, hace una década, habrían sido inimaginables: cámaras conectadas a Internet que permiten publicar imágenes en un solo un clic; sistemas de domótica que controlas las luces, cerraduras de las puertas, sistemas de alarma y monitoreo, aires acondicionados y otros dispositivos del hogar; pulseras que comparten con sus amigos el trayecto de la bicicleta o carrera; electrodomésticos conectados con Internet para regular su funcionamiento; ropa que monitorea la condición física del usuario en tiempo real; etc. Todos estos son ejemplos del IoT, un entorno interconectado, donde toda clase de objetos tienen una presencia digital y la capacidad de comunicarse con otros objetos y personas.

La explosión del IoT rodea a las personas, también, en forma de vehículos, rastreadores de salud inteligentes, detectores de humo y luces acopladas, y prácticamente cualquier otro dispositivo conectado a Internet concepto del cual hay que excluir a los aparatos tradicionales, como el teléfono móvil, tableta o un ordenador.

Los expertos estiman que este año habrá 25 billones de aparatos conectados a Internet y para el año 2020 se estiman 50 billones. Tres millones y medio de sensores ya están en el mercado y se estima que ese número llegue a billones en la próxima década[552]. La cuestión con la creciente utilización de estos dispositivos

---

[551] FTC Staff Report de IoT, de enero de 2015, [en línea], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[552] EVANS, D., "The Internet of Things. How the Next Evolution of the Internet Is Changing Everything", *Cisco Internet Business Solutions Group*, abril 2011, pp. 2-4, [en línea], http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

es que captarán enormes cantidades de información en perjuicio de la privacidad de las personas.

Se estima que la gran cantidad de datos recogidos por los sensores de los aparatos pueden ser procesados mediante tecnología de *Big Data,* las que permitirán hacer patrones y perfiles de las costumbres y hábitos de las personas, información que producirá lesiones a la intimidad.

Parte de una de las respuestas a esto la ha dado la FTC en relación con el informe citado[553], al iniciar un riguroso estudio del tema y las posibles soluciones que deberán implementarse frente a la utilización de esas tecnologías. Debe advertirse que esta no es la primera iniciativa tomada por parte de la FTC en relación al tema, sino que, con anterioridad, había realizado talleres y otros estudios para investigar la forma de hacer frente a esta situación.

Una de las primeras conclusiones a las que llegan los expertos que participaron en la elaboración del informe es que aún no existe una necesidad de emitir o proponer regulaciones sobre el IoT[554], sin embargo, advierten sobre ventajas y desventajas del uso de estos aparatos.

Entre las ventajas señalan los aparatos relacionados con la seguridad, comodidad y la salud de las personas. Algunos aparatos revolucionaros en el área médica, permiten el monitoreo constante de la salud de las personas, como por ejemplo las bombas de insulina, los monitores de pulso y otros signos vitales, esos aparatos pueden registrar, rastrear y monitorear en tiempo real los signos vitales,

---

[553] FTC Staff Report de IoT, de enero de 2015, [en línea], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[554] *Ibid.*

permitiendo a los médicos ajustar los medicamentos o a socorristas enviar ayuda a las personas.

En igual sentido, los aparatos de domótica permiten el monitoreo y ajuste de los electrónicos conectados en el hogar y poder analizar el uso de la energía de los consumidores, a efectos de identificar problemas con los aparatos electrónicos. Algunos fabricantes de vehículos han integrado estos aparatos para mejorar el confort en la conducción y alertar posibles peligros en las vías utilizadas por los conductores, así como problemas con los vehículos, que podrían ser solucionados de forma remota sin necesidad de ir al concesionario.

Los dispositivos IoT también presentan riesgos potenciales en la seguridad de las personas, tales como: usos no autorizados de la información personal; facilitación de ataques de otros sistemas; y la creación de riesgos de seguridad. Aunque todos estos riesgos ya están presentes con el uso de computadoras tradicionales y las redes informáticas, se estima que existe un riesgo mayor con el uso de aparatos IoT.

En primer lugar, hay que advertir que los aparatos que utilizan este tipo de conexiones almacenan una cantidad de información importante de las personas, como, por ejemplo, la información de tarjetas de crédito para hacer compras en línea, en el caso de algunos aparatos de televisión, para poder comprar contenidos. Los sistemas utilizados son más vulnerables que los utilizados en las computadoras, teléfonos y tabletas, lo cual permite una mayor exposición con la posibilidad de posibles ataques.

En segundo lugar, en el caso de dispositivos IoT para uso médico o vehículos, el riesgo es mucho mayor, pues los ataques a estos sistemas, que como ya se indicó son más vulnerables, podrían terminar con la muerte de las personas, por ejemplo, provocar un mal funcionamiento en aparatos que administran insulina, que tomen el control del vehículo o la eliminación de la seguridad de un hogar, todo

esto sin la necesidad de tener contacto físico con los aparatos o las personas y sin introducirse a su domicilio o vehículo.

Ahora bien, también la privacidad de las personas podría verse muy afectada por el IoT, la mayoría de aparatos incluyen cámaras y micrófonos (televisores, vehículos, sistemas de seguridad, etc.) que permiten la expansión de las capacidades de funcionamiento, a lo que se suma la capacidad de almacenamiento de esas informaciones, las cuales contienen datos de la vida privada de las personas como la geolocalización, números de cuentas financieras, información de salud, hábitos y preferencias de consumo, etc.[555]

Según señala Peppet[556], el IoT presentan cuatro retos que se traducen en cuatro problemas legales y son los relativos a la **discriminación**, la **privacidad**, la **seguridad**, y el **consentimiento**. Con relación a la discriminación[557], el citado autor expone que el uso del IoT puede generar nuevas formas de discriminación, incluso las ya protegidas como discriminación étnica, de clases y económica. Explica que la *fusión de sensores* de los aparatos permite obtener información que no es apreciada por el ojo humano, logrando determinar estados de ánimo, problemas psicológicos, o hábitos de consumos de algunas drogas, además de los datos obtenidos del estado general de salud.

---

[555] SCHNEIER, B., *Data and Goliath. The hidden battles to collect yor data and control yor world,* Editorial W.W. Norton & Company, New York, London, 2015, [versión para lector digital Kindle].

[556] PEPPET, S. R., "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", 93 *Texas Law Review*, no. 85, 2014, [en línea], http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf

[557] *Ibíd.,* pp. 117-127.

Con relación a la privacidad[558], el citado autor señala que la utilización de sensores de estos aparatos permitiría obtener una identificación biométrica[559] de las personas, pues dejan una huella única en los registros. Incluso si se suprimiera el nombre, la dirección y el teléfono de las personas sería posible volver a identificar al titular de los datos según los registros almacenados por tales dispositivos. A lo que se suma el hecho de la pequeña capacidad de los aparatos IoT que no cuentan con medidas suficientes para adoptar reglas adecuadas de seguridad. Además, señala el citado autor, representa un reto dar el consentimiento en esos aparatos puesto que no cuentan con pantallas informar al consumidor y este pueda dar el consentimiento sobre las políticas de privacidad. Advierte que aún no se han dictado políticas que alcancen estos problemas en protección del consumidor.

Uno de los problemas más graves es la identificación de información personal. Algunos autores[560] estiman necesario replantear un nuevo concepto con el propósito de proteger entre la información identificada y la información personal identificable (PII) y no la información de identificación. Esto se refiere a la información que no parece estar asociada a un individuo, pero existe una posibilidad remota de que esa información sea re-identificable.

En definitiva, parece que los aparatos IoT ponen a prueba las leyes de privacidad más recientes, frente a nuevas posibilidades de que las empresas obtengan datos de las personas de forma no autorizada, datos con contenido sensible, en los cuales pueden ser identificadas las personas y asociadas a una gran cantidad de datos relacionados con los hábitos, costumbres y condiciones de

---

[558] *Ibíd.,* pp. 128-132.

[559] Puede consultarse el apartado del Capítulo IV apartado 6.3 *supra*.

[560] SCHWARTZ, P. M. y SOLOVE, D. J., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" *New York University Law Review*, vol. 86, New York, 5 de diciembre, 2011, [en línea], http://ssrn.com/abstract=1909366

salud. Adicionalmente, se plantean nuevos retos en el tema de la seguridad de las personas frente a la implementación de esos aparatos en la vida cotidiana. Todas estas situaciones deberán de ser tenidas en cuenta a efectos de incorporarse en las normativas de los países.

2.2.5. Falta de control y asimetría de la información.

Uno de los problemas advertido por el WP29 es la falta de control y asimetría de la información. Comúnmente, la interacción entre objetos, entre objetos y los dispositivos de los individuos, entre individuos y otros objetos y entre objetos y otros sistemas, se traducen en la generación de un flujo de datos que, difícilmente, se pueda gestionar con las herramientas clásicas utilizadas para asegurar la protección de los intereses y derechos de los usuarios[561]. Los datos generados por el IoT no pueden ser revisados de forma adecuada antes de la publicación, lo que sin lugar a dudas generará un riesgo mayor por la falta de control y auto exposición de manera excesiva en perjuicio de los usuarios, lo que se agrava ante la posibilidad de los aparatos de comunicarse con otros de forma automática y por defecto.

La falta o imposibilidad de control del flujo de datos por parte de los usuarios pondrá en riesgo su derecho a la intimidad, situación que además se verá afectada por el crecimiento de la computación en la nube (*cloud computing*) y el *Big Data*.

[561] WP29, Dictamen 8/2014, sobre la reciente evolución del Internet de las cosas, de 16 de setiembre de 2014, [en línea], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

2.2.6. Calidad del consentimiento del usuario.

Uno de los principales desafíos que tienen los gobiernos frente a la protección de datos personales, se refiere a la calidad del consentimiento informado que se exige a los usuarios por parte de las empresas de productos y servicios.

Es tangible el problema relacionado con la falta de información sobre el consentimiento informado. Según la citada opinión[562], ello constituye una verdadera barrera para demostrar el consentimiento válido, según se establece en la legislación comunitaria.

En la propuesta del nuevo Reglamento[563], se añade a la definición de consentimiento el criterio *explícito*[564], para evitar un paralelismo o confusión con el consentimiento *inequívoco,* con el fin de dotar una definición única y coherente que garantice que el interesado es consciente de que otorga su consentimiento, para qué y para cuáles efectos. Así mismo, en los artículos 6 y 7 se aclaran las condiciones para que el consentimiento sea válido como fundamento jurídico del tratamiento lícito[565].

En ese sentido, el considerando 25[566] de la citada propuesta, señala que se debe dar el consentimiento de forma explícita, por cualquier medio apropiado que

---

[562] *Ibíd.*

[563] Propuesta del Reglamento General de Protección de Datos de la U.E., [en línea], http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=es

[564] Art. 4.8 de la Propuesta del Reglamento General de Protección de Datos de la U.E., [en línea], http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=es

[565] Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento de la persona interesada o sobre alguna otra base legítima establecida por ley, ya sea en el Reglamento propuesto o en otros actos legislativos del Estado miembro o de la Unión.

[566] Considerando 25 de la Propuesta del Reglamento General de Protección de Datos de la U.E., [en línea], http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=es

permita la manifestación libre, específica e informada de la voluntad del interesado, ya sea mediante una declaración o una clara acción afirmativa, la cual garantice que la persona es consciente de que está dando su consentimiento al tratamiento de datos personales, incluso mediante la selección de una casilla de un sitio web en internet o cualquier otra declaración o conducta que indique, en forma clara, que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo fin o fines. Si el consentimiento del interesado se ha de dar a raíz de una solicitud electrónica, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

Como se describe también en el Dictamen 02/2013 del WP29[567] sobre aplicaciones en los dispositivos inteligentes, la computación portátil además pone de relieve los desafíos derivados de la continua recopilación de datos de otros en las cercanías y por períodos prolongados de tiempo.

Según se afirma en el Dictamen 8/2014 del WP29[568], los mecanismos clásicos utilizados para obtener el consentimiento de los individuos pueden ser difíciles de aplicar en la IoT, lo que resulta en un consentimiento "de baja calidad" o de bajo estándar, sustentado en la falta de información o la imposibilidad fáctica por parte de los individuos para dar su consentimiento adecuado con el fin de expresar esas preferencias, lo anterior en razón de la utilización de sensores que utilizan los aparatos para dar información a terceros sin el consentimiento del usuario.

---

[567] WP29, Dictamen 02/2010 de 27 de febrero de 2013, [en línea], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf

[568] WP29, Dictamen 8/2014, sobre la reciente evolución del Internet de las cosas, de 16 de setiembre de 2014, [en línea], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

2.2.7. Patrones y perfiles de la información relacionados con los hábitos y costumbres de las personas.

Tal y como se ha comentado, piezas aisladas de la información de las personas, posibilitan la creación de perfiles y patrones de sus hábitos, costumbres y preferencias de las personas. El análisis basado en la información, atrapados en un entorno IoT, podría permitir la detección de patrones de vida y de comportamiento aún más detallados y completos de un individuo.

2.2.8. La privacidad frente al uso de aviones no tripulados (*drones*).

Las tecnologías han logrado una penetración impactante en la sociedad, permitiendo el acceso a instrumentos que con anterioridad solo era posible al personal de agencias de inteligencia secreta para hacer espionaje de los enemigos. Es común encontrar aparatos de uso cotidiano con cámaras ocultas como luces, detectores de humo, lapiceros, relojes, entre otros artículos, que permiten a la población civil acceder a sofisticados instrumentos para lograr grabaciones en su vida cotidiana. Los drones o aviones no tripulados constituyen otros aparatos que se presentan como un nuevo producto de consumo, que permiten llevar a los cielos cámaras de video para los entusiastas del aeromodelismo y la fotografía.

Estos nuevos aparatos del espacio aéreo reciben diversos nombres, tales como drones, RPAs (por sus siglas en inglés, *Remotely Piloted Aircaft*) o UAVs (por sus siglas en inglés, *Unmanned Aerial Vehicle*). La reducción en el precio de estas tecnologías ha generado una venta descontrolada y una verdadera moda, que ahora presenta un desafío para la seguridad aérea y para la intimidad de las personas.

De nuevo el desarrollo de esas tecnologías y la facilidad en el acceso ha generado la necesidad de regulación jurídica para el uso y operación de las aeronaves civiles pilotadas por control remoto. Por esa razón en España se ha

aprobado el Real Decreto 18/2014 de 15 de octubre[569], dedicado a medidas urgentes para regular el crecimiento, la competitividad y la eficiencia dirigidas a "fomentar el funcionamiento eficiente de los mercados, mejorar la financiación y la empleabilidad" en el cual se establece el régimen específico de las operaciones de las aeronaves civiles pilotadas por control remoto.

Entre las razones para establecer el marco jurídico aplicable a las operaciones de las aeronaves civiles pilotadas por control remoto se tienen: la necesidad de dotar de un marco jurídico en condiciones de seguridad que permita el desarrollo del sector tecnológico, en el que se considere el actual contexto económico. Y que se tomen las medidas para diversificar la actividad económica y potenciar la actividad industrial, en beneficio de la economía y el empleo.[570]

En definitiva, la regulación responde a la necesidad de dotar de un marco jurídico a un sector que carece de disposiciones específicas. Por lo cual resulta necesario garantizar la seguridad de las operaciones aéreas y de las personas y bienes subyacentes, con el propósito de permitir la operación de estas aeronaves en condiciones de seguridad y su control por la Agencia Estatal de Seguridad Aérea, para evitar riesgos de seguridad que pueden provocar accidentes o incidentes de aviación.

Bajo esta regulación se atribuye a los Ministerios de Defensa y Fomento la competencia conjunta en materia de política y estrategia para la estructuración y gestión del espacio aéreo, así como la adopción de las medidas específicas en este ámbito. Al Ministerio de Fomento se atribuye la determinación de las condiciones o

---

[569] Real Decreto 18/2014 de 15 de octubre, [en línea], https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-10517

[570] *Vid.* Considerando V del Real Decreto 18/2014 de 15 de octubre.

restricciones de uso del espacio aéreo, para la circulación aérea general, ante situaciones de crisis ordinarias generadas por fenómenos naturales, accidentes o cualquier otra circunstancia similar, reservando al Ministerio de Defensa las competencias sobre la materia en situaciones extraordinarias o de emergencia declaradas por el Presidente del Gobierno o el Ministerio de Defensa.[571]

Particularmente en el artículo 50 de la citada normativa se establecen las condiciones generales para regular la actividad de las aeronaves civiles pilotadas por control remoto, y se agrega que mientras no entre en vigor la norma reglamentaria prevista en la Disposición final segunda, apartado 2, de esa Ley, las operaciones de aeronaves civiles pilotadas por control remoto quedan sujetas a lo establecido en este artículo.[572]

De la citada normativa interesa resaltar lo que señala en el apartado primero del artículo 50, en el cual se indica que, "*de lo dispuesto en este artículo no exime al operador, que es, en todo caso, el responsable de la aeronave y de la operación, del* ***cumplimiento del resto de la normativa aplicable****, en particular en relación con el uso del espectro radioeléctrico,* ***la protección de datos o la toma de imágenes aéreas****, ni de su responsabilidad por los daños causados por la operación o la aeronave*."[573] Se puede apreciar que la disposición no exime al operador remoto de las aeronaves del cumplimiento de las leyes relacionadas con la protección de datos e intimidad, sin embargo, se extraña una referencia más adecuada para la protección de estos derechos, en la cual se establezcan los mecanismos de protección, los derechos a proteger y las entidades encargadas de

---

[571] *Ibid.*

[572] *Vid.* Art. 50 del Real Decreto 18/2014 de 15 de octubre.

[573] Art. 50.1 párrafo 2° del Real Decreto 18/2014 de 15 de octubre.

resolver los problemas relacionados con la utilización y operación de los drones y la protección de la intimidad de otras personas.

En el supuesto que se esté ante la vulneración del derecho a la intimidad o protección de datos personales por medio de la utilización de un drone, ¿cuál sería el procedimiento para formular una denuncia ante la autoridad competente?, es decir, ¿qué debería hacer una persona en esta condición? Ya en EE.UU. se han presentado casos en los cuales las personas han reaccionado de forma violenta ante la intrusión de un RPA en el espacio aéreo ubicado sobre su propiedad, situación que finalmente fue resuelta a favor del operador del artefacto, quien resultó indemnizado por parte de su vecino que derribó el drone con un arma de fuego. En este caso no se consideraron las posibles afectaciones a la privacidad del atacante, en lugar de eso, también se inició el proceso por haber disparado al aire en una zona poblada con el propósito de derribar la aeronave que sobrevolaba su propiedad, por la puesta en peligro de la población.[574]

Lo anterior solo tienen el propósito de ejemplificar la necesidad de una adecuada regulación sobre el uso de artefactos que pueden surcar los cielos y obtener imágenes y videograbaciones de lugares a los cuales no se podría tener acceso por tierra. La justicia de propia mano fue la que imperó en la situación señalada y un exceso en la defensa por parte de la víctima terminó en un proceso en el cual le declaró responsable de la indemnización por daños y perjuicios causados al operador del drone y la responsabilidad penal por disparar al aire en zona poblada.

---

[574] *Vid.* ERNST, D., "Ky. man arrested after shooting down $1,800 drone hovering over sunbathing daughter" en *The Washingtontimes*, 30 de julio de 2015, [en línea], http://www.washingtontimes.com/news/2015/jul/30/william-merideth-arrested-after-shooting-down-1800/

En EE.UU. la Administración Federal de Aviación (FAA) ha iniciado una campaña con asocio de organizaciones privadas, para fomentar la seguridad en materia de vuelos no tripulados y con ello da a conocer una propuesta para la reglamentación[575] de estas actividades. En la propuesta se reconoce, por parte de la FAA, que la utilización de estos aparatos puede poner en riego los derechos civiles y a la privacidad y libertad de las personas. Sin embargo, una organización no gubernamental, *The Electronic Privacy Information Center* (EPIC), interpuso una demanda contra la FAA, por la falta de regulación de la privacidad en el proyecto propuesto[576]. Esta demanda fue respaldada por una serie de organizaciones y expertos en privacidad.

En Costa Rica también se han manifestado las preocupaciones relacionadas con la falta de regulación con respecto a la utilización de aeronaves UAVs y RPAs. Sin embargo, las autoridades de aviación trabajaron desde hace año y medio en una reglamentación general en la cual se discipline el uso y registro de estos aparatos. Entre tanto no entre en vigencia la normativa aprobada el pasado 17 de setiembre de 2015, la Dirección General de Aviación Civil emitió una reglamentación básica[577] en la cual se indican las restricciones y limitaciones para vehículos aéreos no tripulados. Lamentablemente en esta se omite algún señalamiento acerca de la protección a la privacidad e intimidad de las personas.

---

[575] Department of Transportation, Federal Aviation Administration, 14 CFR Parts 21, 43, 45, et al., Operation and Certification of Small Unmanned Aircraft Systems; Proposed Rule, [en línea], http://www.gpo.gov/fdsys/pkg/FR-2015-02-23/pdf/2015-03544.pdf

[576] La demanda puede ser consultada en: https://epic.org/privacy/litigation/apa/faa/drones/EPIC-v-FAA-DC-Cir-Petition.PDF

[577] Dirección General de Aviación Civil, restricciones y limitaciones de operación para vehículos aéreos no tripulados, 08 de mayo de 2015, [en línea], http://www.dgac.go.cr/Aeronaves%20no%20Tripuladas/cc05_15%20opr%20drones%20AIC.pdf

Si bien se reconoce la utilidad de los UAVs y RPAs para fines comerciales, científicos, humanitarios, de atención de emergencias y otros, también pueden ser instrumento para la perpetración de crímenes[578] e invasiones a la privacidad de las personas, al permitir accesos que antes eran poco probables a través de los medios existentes. En el proyecto del reglamento se prevé la prohibición para el uso de estas aeronaves, por razones de seguridad y privacidad, sobre aglomeraciones humanas, de edificios, barrios o casas, ni a menos de 30 metros de una persona, inmueble o vehículo.

El reglamento para la operación de RPAs y UAVs, propuesto en Costa Rica, pretende cumplir los lineamientos generales e instrumentos jurídicos definidos por la Organización de Aviación Civil Internacional (OACI)[579]. En este proyecto para reglamentar la actividad se pretende una protección de los datos y la privacidad de las personas y, según las autoridades se espera que entre en funcionamiento a finales del año 2015.

Hoy en día no se duda sobre el beneficio que ofrecen a la población este tipo de artefactos, sin embargo, será necesaria la implementación de medidas que protejan la privacidad de las personas y se incluyan los procedimientos y mecanismos legales, en los cuales se determinen los procedimientos en los casos de vulneración de los derechos de las personas.

---

[578] Las autoridades de Ohio (EE.UU.) confirmaron que un drone introdujo un paquete con drogas en una prisión estatal en julio de 2015. ORTIZ, E., "Drone Drops Drugs Into Mansfield, Ohio, Prison, Prompts Yard Brawl: Report", en *NBCNEWS*, 5 de agosto de 2015, [en línea], http://www.nbcnews.com/news/us-news/drone-drops-drugs-mansfield-ohio-prison-prompts-yard-brawl-report-n404426

[579] Organización de Aviación Civil Internacional, consultable en: http://www.icao.int/about-icao/Pages/default.aspx

De esta manera, mediante la Directiva Operacional DO-002-OPS-RPAS[580], la Dirección General de Aviación Civil, emite una regulación en la cual se establecen las normas básicas para la operación con sistemas de aeronaves piloteadas a distancia (RPAs), con el propósito de garantizar que la actividad mantenga una seguridad operacional parecida a la actividad de la aviación civil convencional, lo anterior de conformidad con los estándares establecidos por la OACI.

De esta manera en la señalada normativa, específicamente en el apartado 11 se establece que "*Los propietarios u operadores de Aeronave Piloteada a Distancia (RPA), deben de cumplir con las disposiciones establecidas en el marco jurídico nacional en lo relativo a la protección de datos y el derecho a la privacidad*"[581] y señal de forma específica el marco jurídico de protección de este derecho[582].

Asimismo, se establece un mecanismo de denuncia por la captación y difusión de imágenes ante la Dirección General de Aviación Civil, para los casos en los cuales estas se realicen sin el consentimiento del titular.

En caso que se compruebe la captación y difusión de imágenes sin el consentimiento del titular, la Dirección General de Aviación Civil podría imponer la sanción de cancelación del certificado de explotación de aeronave piloteada a distancia (RPAs) de conformidad con el artículo 13 y siguientes de la Ley General de Aviación Civil. Se debe aclarar que la cancelación de este certificado no exime

---

[580] Directiva Operacional DO-002-OPS-RPAS de la Dirección General de Aviación Civil de 31 de agosto de 2015, [en línea], http://www.dgac.go.cr/Aeronaves%20no%20Tripuladas/Directiva%20Operacional%20DO-002-OPS-RPAS.pdf

[581] *Ibíd.,* apartado 11.

[582] Arts., 23 y 24 de la CPC, art. 8.g. de la Declaración Universal de los Derechos Humanos y el Código Penal, Ley No. 4573 Publicada en el Alcance 120 a La Gaceta N° 257 de 15 de noviembre de 1970 y el Art. 13.2 de la Convención Interamericana de Derechos Humanos.

de la responsabilidad de las personas en el ámbito jurisdicciones por las violaciones a los derechos relacionados con la intimidad.

Se estima que la creación de registros para la inscripción de RPAs y UAVs será una medida conveniente a fin de regular la actividad, pero siempre quedarán aparatos de menor capacidad fuera de este registro, los cuales aún permiten la captura de imágenes que, sin lugar a dudas, con el tiempo mejorarán sus capacidades y con ello se favorecerá la vulneración de la privacidad de las personas.

2.3. Principios de la autodeterminación informativa en la LOPD.

En el Título II de la LOPD (arts. 4-12), se indican los principios de la protección de datos, los cuales deben cumplirse para que el tratamiento de datos por parte de terceros se considere lícito y legítimo[583]:

La calidad de los datos[584]. En este sentido se hace referencia a que solo podrán recogerse los datos para su tratamiento, cuando sean adecuados, pertinentes y no excesivos para la finalidad determinada, explícita y legítima que origine su obtención.

Derecho de información[585]. Los titulares de los datos deberán ser informados de forma previa, de modo expreso, preciso y sin dar lugar a

---

[583] *Cfr.* Art. 5 de la Propuesta del Reglamento General de Protección de Datos de la U.E., [en línea], http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=es; en este se indican los principios relacionados con el tratamiento de los datos personales y los presenta de la siguiente forma: a) tratados de manera lícita, leal y transparente en relación con el interesado; b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines; c) adecuados, pertinentes y limitados al mínimo necesario en relación a los fines para los que se traten; solo se tratarán si y siempre que estos fines no pudieran alcanzarse mediante el tratamiento de información que no implique datos personales; d) exactos y se mantendrán actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin demora los datos personales que sean inexactos con respecto a los fines para los que se tratan; e) conservados en una forma que permita identificar al interesado durante un período no superior al necesario para lo fines para los que se someten a tratamiento; los datos personales podrán ser conservados durante períodos más largos, siempre que se traten exclusivamente para fines de investigación histórica, estadística o científica, con arreglo a las normas y condiciones establecidas en el artículo 83 y si se lleva a cabo una revisión periódica para evaluar la necesidad de seguir conservándolos; f) tratados bajo la responsabilidad del encargado o responsable del tratamiento, quien, para cada operación de tratamiento, garantizará y demostrará el cumplimiento de las disposiciones del presente Reglamento.

[584] Art. 4 LOPD.

[585] Art. 5 LOPD.

equivocaciones de la existencia de un fichero o almacenamientos de sus datos, sobre la finalidad de la recogida de estos datos y de los destinatarios de la información. Además, se les deberá informar de la identidad y dirección del responsable del fichero, y de la posibilidad de ejercer su derecho de acceso[586], rectificación, cancelación[587] y oposición[588] (derechos ARCO).

Consentimiento del afectado[589]. Salvo excepciones legales, el tratamiento de los datos personales requerirá el consentimiento inequívoco del afectado, que puede ser tácito o expreso, dependiendo de si los datos que se pretenden recabar están o no protegidos de forma especial. No obstante, la LOPD, especifica los casos en los que no será preciso el consentimiento, siempre preservando los derechos y libertades fundamentales del titular.

Datos especialmente protegidos[590]. Se consideran datos especialmente protegidos, también denominados sensibles, aquellos que revelen la ideología, afiliación sindical, religión, creencias, origen racial, de la salud y la vida sexual de la persona los cuales podrán ser recabados, tratados y cedidos cuando así lo disponga una ley, o por razones de interés general, siempre con el consentimiento expreso del interesado. Los datos relativos a comisiones de infracciones penales o administrativas, también se consideran sensibles.

---

[586] Art. 15 de la LOPD y arts. 27 a 30 del Real Decreto 1720/2007.

[587] Art. 16 de la LOPD y en los arts. 31 a 33 del Real Decreto 1720/2007.

[588] Arts. 35 y 36 del Real Decreto 1720/2007.

[589] Art. 6 LOPD.

[590] Arts. 7 y 8 LOPD.

Seguridad de los datos[591]**.** Este principio implica al responsable del fichero, y en su caso, al encargado del tratamiento quienes deben habilitar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar la alteración, pérdida, tratamiento o acceso no autorizado. Utilizarán las herramientas adecuadas para asegurar el perfecto estado de la tecnología, tanto por la naturaleza de los datos almacenados como por los riesgos que comporta su tratamiento, ya sean provocados por la acción humana o por el medio físico o natural de los locales, equipos, sistemas o programas que se utilicen en los centros de tratamiento de datos.

Deber de secreto[592]**.** Norma de conducta fundamental del responsable del fichero y de quienes intervengan en cualquier fase del tratamiento de los datos. Incluso, esta obligación subsistirá, aunque se extinga su relación con el responsable del fichero.

Comunicación de los datos[593]**.** Solo podrán comunicarse los datos de carácter personal objeto del tratamiento a un tercero, para el cumplimiento de fines relacionados, directamente, con las funciones legítimas tanto de quien los cede como de quién los recibe, con el previo consentimiento del interesado, salvo que sean cesiones autorizadas por ley, se trate de datos recogidos de fuentes accesibles al público, o cuando se produzca entre administraciones públicas o en otros casos regulados en el apartado 2 y ss. del artículo 11 de la LOPD.

Acceso a los datos por cuenta de terceros[594]**.** No se considerará comunicación de datos el acceso de un tercero cuando dicho acceso sea necesario

---

[591] Art. 9 LOPD.

[592] Art. 9 LOPD.

[593] Art. 11 LOPD.

[594] Art. 12 LOPD.

para la prestación de un servicio al responsable del tratamiento. Cuando se realicen tratamientos por cuenta de terceros, siempre se formalizará mediante un contrato, por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose de forma expresa que el encargado del tratamiento tratará los datos únicamente, según las instrucciones del responsable y que no los aplicará o utilizará para fines distintos de los contratados, ni los comunicará a otras personas, ni siquiera para su conservación. Caso de incumplimiento, deberá responder de las infracciones en las que hubiere podido incurrir personalmente.

3. DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN Y OLVIDO O SUPRESIÓN.

3.1. En los Estados Unidos de América.

En general el derecho de acceso a la información es una de las garantías del derecho a la autodeterminación informativa, que permite a cualquier persona el acceso a los datos que le conciernan y sean de objeto de tratamiento, lo anterior para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento, así como también implica el derecho de las personas, rectificar o solicitar la cancelación de los datos.

En EE.UU. no existe un derecho de acceso a los datos personales en la mayoría de leyes de privacidad. Con excepción de la HIPAA[595] y algunas leyes del Estado de California, no se ofrece a los interesados el derecho de acceso a sus datos personales. Una excepción se encuentra en la COPPA[596], que permite a los padres ver la información personal recogida por un sitio web acerca de un menor, otorgándole la posibilidad de eliminar o corregir dicha información.

En el caso de la HIPAA, las personas pueden obtener acceso a sus registros sanitarios y podrían solicitar la corrección y eliminación de información (con algunas excepciones), y obtener el registro de la información utilizada o revelada.

---

[595] Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat 1936, [en línea], http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf

[596] Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. § 6501–6505, [en línea], https://www.law.cornell.edu/uscode/text/15/chapter-91

De otra parte la GLB[597] permite a los consumidores o clientes darse de baja (*opt-out*) de ciertas revelaciones, pero no proporciona el derecho relativo al acceso de los datos personales.

La California Shine the Light Law[598] permite a los consumidores enterarse de los casos en que su información personal es compartida por parte de las empresas con fines de mercadeo y anima a las empresas a no utilizar estas prácticas. Ante la solicitud de un cliente, la empresa debe proporcionar una lista de las categorías de información personal divulgada a otras empresas para sus fines de mercadeo durante el año calendario, con los nombres y direcciones de las empresas. El usuario posee la potestad de retirar la información que ha sido compartida con otras empresas.

En sentido similar, se encuentran reguladas las compañías financieras a través del California's Financial Information Privacy Act y en el caso de los estudiantes en el California's student privacy law, que prohíbe acumular información para hacer perfiles de los estudiantes o sus padres.

Hasta ahora ese es el panorama de los EE.UU. con respecto a la protección de los datos de las personas, sin embargo, nuevas propuestas y lineamientos están en proceso de ser aprobadas. Dos de estos son en particular de suma importancia, desde el mes de marzo de 2011, la Unión Europea ha estado negociando con los Estados Unidos un acuerdo internacional marco denominado "***Data Protection***

---

[597] Gramm-Leach-Bliley (GLB) Act of 1999, 12 U.S.C. § 1811, [en línea], https://www.law.cornell.edu/uscode/text/12/1811

[598] California Shine the Light Law Civil Code §§1798.83 of XX, [en línea], http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

Umbrella Agreement"[599] con el propósito de proteger la transferencia de datos personales entre la U.E. y EE.UU. con fines policiales. Esto incluye los casos en los que los datos personales son enviados de UE a los EE.UU. para la prevención, detección, investigación y enjuiciamiento de las infracciones penales, incluido el terrorismo.

Según un comunicado[600] del Comisionado de Datos de 24 de junio de 2015, este convenio proporcionará a las empresas normas comunes modernas que se aplican a todos los servicios que prestan en la U.E. También eliminará trámites innecesarios, tales como procedimientos de notificación, reducirá los costos y aplicará conceptos modernos como la privacidad desde el diseño y el enfoque basado en el riesgo. Será tecnológicamente neutral y no cerrará las puertas a futuras innovaciones.

De otra parte, el 23 de febrero de 2012[601], presentó un informe para el desarrollo de una ley para proteger la privacidad de los consumidores en línea denominado ***Privacy Bill of Rights Act of 2015[602]****,* como parte de un plan integral para mejorar la protección de la privacidad de los consumidores y garantizar que

---

[599] Actualmente, la Comisión está negociando un acuerdo marco entre la U.E. y EE.UU. sobre la protección de los datos personales transferidos en cumplimiento de la ley. El acuerdo marco será un acuerdo internacional sobre la base del artículo 218 del TFUE, y tendrá prioridad sobre la legislación secundaria de la U.E. Las negociaciones se llevan a cabo a puerta cerrada, y los documentos son confidenciales. El Parlamento Europeo tendrá que dar su aprobación al acuerdo, pero no tiene el poder para decidir suspender o terminar el acuerdo.

[600] Palabras del Comisionado Jourová después de la puesta en marcha de la regulación diálogo a de protección de datos, Bruselas, 24 de junio 2015, [en línea], http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm

[601] Informe para la aprobación de la ley de privacidad de los datos de los consumidores (Privacy Bill of Rights Act), febrero 2012, [en línea], https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[602] Privacy Bill of Rights Act of 2015, proyecto de ley, [en línea], https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf

Internet siga siendo un motor para la innovación y el crecimiento económico. El plan guiará los esfuerzos para dar a los usuarios más control sobre cómo se usa su información personal en Internet y para ayudar a las empresas a mantener la confianza de los consumidores y crecen en el entorno digital que cambia rápidamente. Si bien esta normativa está dirigida al comercio, lo cierto es que se propone como indispensable para proteger la privacidad de las personas y los datos personales en línea. Permite el acceso y control de la información personal y otros principios tales como:

Control individual: Los consumidores tienen derecho a ejercer el control sobre lo que las empresas de datos personales recogen de ellos y cómo lo utilizan.

Transparencia: Los consumidores tienen derecho a la información fácil, comprensible y accesible sobre las prácticas de privacidad y seguridad.

Respeto de uso: Los consumidores tienen derecho a que las empresas que recopilan, usan y divulgan datos personales sean consecuentes con el contexto en el que se proporcionaron los datos.

Seguridad: Los consumidores tienen derecho al manejo seguro y responsable de los datos personales.

Acceso y precisión: Los consumidores tienen derecho a acceder a los datos personales correctos en formatos utilizables, de una manera que sea apropiada a la sensibilidad de los datos y el riesgo de consecuencias adversas para ellos si los datos son inexactos.

Colección enfocada y uso responsable: Los consumidores tienen derecho a imponer límites razonables a los datos personales que las empresas recogen y conservan.

Responsabilidad: Los consumidores tienen derecho a que los datos personales recogidos por las empresas sean tratados con las medidas apropiadas

para asegurar que se adhieren a la Declaración de Derechos de Privacidad del Consumidor.

3.2. En Europa y España.

3.2.1. Derecho de acceso a los datos personales.

La Directiva 95/46/CE relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos de 24 de octubre de 1995, en el artículo 12[603], dispone del derecho de acceso del interesado a los datos. En el cual los Estados miembros deberán de garantizar a todos los interesados el derecho de obtener del responsable del tratamiento:

a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información, por lo menos, de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;

- la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;

- el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

---

[603] *Vid.* Art. 12 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.

De modo muy similar, en el artículo 15 de la LOPD[604], se garantiza el derecho de acceso a la información, mediante el cual el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. Así mismo, la información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes. En el artículo 27 del Reglamento de la LOPD se dispone el derecho de acceso y en el artículo 28 el ejercicio de este derecho[605].

Consecuentemente, este derecho de acceso facilita al interesado la aproximación o el acercamiento al contenido del tratamiento de la información personal de él recogida, de forma que pueda conocer y por tanto valorar la calidad de los datos personales, y el respeto al principio de finalidad, ya que con la mera consulta del fichero no puede accederse a un conocimiento sustantivo y completo del tratamiento. Por tanto, se establece, mediante el acceso a la información

---

[604] *Cfr.* Art. 15 de la LOPD.

[605] *Vid.* Arts. 27 y 28 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado mediante Real Decreto 1720/2007.

personal, el ejercicio de otros derechos o garantías individuales de la persona imprescindibles para la protección de sus datos personales. Pareciera un derecho instrumental a través de cual podrán ejercerse otros derechos como el de rectificación o cancelación[606].

Conviene que se mencione que en la Propuesta de Reglamento General de Protección de Datos de la U.E.[607], el derecho de acceso si bien se basa en la letra del artículo 12 de la Directiva 95/46/CE, en el artículo 15 dispone el derecho de acceso del usuario a sus datos personales y añade nuevos elementos, como la obligación de informar a los interesados sobre el periodo de conservación, los derechos de rectificación y supresión y a interponer una reclamación, así como también se refuerzan estos derechos para permitir un mejor control de los datos personales cuando son sometidos al tratamiento por medios electrónicos.

3.2.2. Derechos de rectificación, cancelación, oposición y olvido o supresión.

La Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos de 24 de octubre de 1995, señala los principios reactivos a la calidad de los datos en el artículo 6.1.d)[608] al disponer que, "*Los Estados miembros dispondrán que los datos personales sean: …d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que*

---

[606] *Cfr.* HERRÁN ORTÍZ, A. I., *op. cit.,* [biblioteca electrónica Vlex].

[607] *Vid.* Art. 15 de la Propuesta del Reglamento General de Protección de Datos de la U.E..

[608] *Vid.* Art. 6.1.d) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

fueron tratados posteriormente, sean suprimidos o rectificados", estableciendo el derecho a la rectificación o supresión de los datos para que ello sea adoptado en la normativa de los Estados miembros. Este derecho incluye la condición de que, al momento de requerir los datos, se informe al interesado la existencia de derecho de acceso y rectificación de los datos que le conciernen[609].

De igual forma se indica en el artículo 12.b)[610] que se debe garantizar a los interesados el derecho de obtener un tratamiento responsable de los datos de su interés, incluida la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos.

En el apartado anterior, relativo al derecho de acceso a la información de los datos personales por parte de los titulares, se había indicado que en la Propuesta de Reglamento General de Protección de Datos de la U.E.[611], el derecho de acceso si bien se basa en la letra del artículo 12 de la Directiva 95/46/CE, en el artículo 15 dispone el derecho de acceso del interesado a sus datos personales y se mencionan, específicamente, los derechos de rectificación y supresión en el artículo 16[612].

---

[609] *Vid.* Arts. 10.1.c) y 11.1.c) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

[610] *Vid.* Arts. 12.b) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

[611] *Vid.* Arts. 15 y 16 de la Propuesta del Reglamento General de Protección de Datos de la U.E.

[612] En el artículo 16 de la Propuesta del Reglamento General de Protección de Datos de la U.E., se indica: "*El interesado tendrá derecho a obtener del responsable del tratamiento la rectificación de los datos personales que le conciernen cuando tales datos resulten inexactos. El interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos, en particular mediante una declaración rectificativa adicional*".

La citada Propuesta de Reglamento General de Protección de Datos de la U.E., contempla en el artículo 17 el derecho al olvido y a la supresión de datos personales. Esto implica algunas mejoras importantes con respecto al tratamiento que se señalaba en la Directiva 95/46/CE, puesto que, si bien se garantizaba el derecho de la rectificación de los datos y la supresión, ahora en esta propuesta se precisa con más detenimiento las condiciones para hacer valer estos derechos.

Según esta normativa[613] el interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en lo que respecta a los datos personales proporcionados por el interesado siendo niño, cuando concurra alguna de las circunstancias siguientes: a) que los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados; b) que el interesado retire el consentimiento en que se basa el tratamiento, de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a) (consentimiento informado), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos; c) que el interesado se oponga al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19 (derecho de oposición); y, d) que el tratamiento de datos no sea congruente con el presente Reglamento por otros motivos. Este artículo se refiere al derecho a que sean suprimidos los datos personales en las condiciones señaladas.

En ese mismo sentido llama la atención el art. 17.2 de la citada propuesta[614] al obligar al responsable del tratamiento de datos personales a que, en caso de publicación de esos datos, adopte todas las medidas razonables, incluidas medidas técnicas, en lo que respecta a los datos de cuya publicación sea responsable, con miras a informar a los terceros que estén tratando dichos datos a que un interesado

---

[613] *Cfr.* Art. 17.1 de la Propuesta del Reglamento General de Protección de Datos de la U.E.

[614] *Vid.* Propuesta del Reglamento General de Protección de Datos de la U.E.

les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. Cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de esa publicación.

También se establecen salvedades[615] para que los responsables puedan mantener datos personales, cuando tal conservación resulte necesaria, ya sea: a) para el ejercicio del derecho a la libertad de expresión, de conformidad con lo dispuesto en el artículo 80; b) por motivos de interés público en el ámbito de la salud pública, de conformidad con lo dispuesto en el artículo 81; c) con fines de investigación histórica, estadística y científica, de conformidad con lo dispuesto en el artículo 83; d) para el cumplimiento de una obligación legal de conservar los datos personales impuesta por el Derecho de la Unión o por la legislación de un Estado miembro a la que esté sujeto el responsable del tratamiento; las legislaciones de los Estados miembros deberán perseguir un objetivo de interés público, respetar la esencia del derecho a la protección de datos personales y ser proporcionales a la finalidad legítima perseguida; y e) en los casos contemplados en el apartado 4.

El responsable de los datos puede limitar[616] el tratamiento de los datos personales cuando: a) el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los datos; b) el responsable del tratamiento ya no necesite los datos personales para la realización de su misión, pero estos deban conservarse a efectos probatorios; c) el tratamiento sea ilícito y el interesado se oponga a su supresión y solicite en su lugar la limitación de su uso; y, d) el interesado solicite la transmisión de los datos personales a otro sistema de tratamiento automatizado, de conformidad con lo dispuesto en el artículo

---

[615] *Cfr.* Art. 17.3 de la Propuesta del Reglamento General de Protección de Datos de la U.E.

[616] *Cfr.* Art. 17.4 de la Propuesta del Reglamento General de Protección de Datos de la U.E.

18, apartado 2. Según el apartado 5 del artículo citado, los datos personales contemplados en el apartado 4 solo podrán ser objeto de tratamiento para efectos probatorios, o con el consentimiento del interesado, o con miras a la protección de los derechos de otra persona física o jurídica o en pos de un objetivo de interés público[617].

De igual forma, cuando el tratamiento de esos datos se encuentre limitado bajo alguna de las causas del apartado 4, el responsable del tratamiento deberá de informar al interesado antes de levantar la limitación al tratamiento[618].

Otra de las responsabilidades de quien trata los datos será la de implementar mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales o para el examen periódico de la necesidad de conservar los datos[619].

Una vez que los datos han sido suprimidos, el responsable de su tratamiento no podrá dar ninguna otra forma de tratamiento a los datos[620].

Por último, se debe indicar que se dejó a la Comisión[621] la facultad de adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar: a) los criterios y requisitos relativos a la aplicación del apartado 1 en sectores y situaciones específicos de tratamiento de datos; b) las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público, a que se refiere el apartado 2; y, c)

---

[617] *Cfr.* Art. 17.5 de la Propuesta del Reglamento General de Protección de Datos de la U.E.

[618] *Cfr.* Art. 17.6 de la Propuesta del Reglamento General de Protección de Datos de la U.E.

[619] *Cfr.* Art. 17.7 de la Propuesta del Reglamento General de Protección de Datos de la U.E.

[620] *Cfr.* Art. 17.8 de la Propuesta del Reglamento General de Protección de Datos de la U.E.

[621] *Cfr.* Art. 17.9 de la Propuesta del Reglamento General de Protección de Datos de la U.E.

los criterios y condiciones para limitar el tratamiento de datos personales contemplados en el apartado 4.

Se puede apreciar, claramente, que la propuesta de Reglamento introduce una considerable mejora de los derechos de acceso, rectificación y cancelación de datos personales a nivel europeo, fijando plazos de respuesta a las peticiones de las personas afectadas, autorizando el ejercicio de estos derechos por vía electrónica y obligando a motivar las denegaciones.

En España los derechos de rectificación y cancelación están dispuestos en la LOPD, específicamente en el artículo 16, el que señala:

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Este derecho de rectificación se traduce en la facultad del interesado para solicitar la corrección de datos que sean incompletos o inexactos. No se trata de un derecho que se conceda a los particulares como un beneficio abstracto de la información veraz, ya que a un sujeto que no se encuentre afectado carece de legitimación para justificar su intromisión en la libertad de información de otra persona.

El significado del derecho de rectificación ha sido confirmado por la interpretación que ha efectuado el Tribunal Constitucional Español, al declarar que no es preciso que quien rectifique acredite la veracidad de la rectificación, sino que se trata de permitir a una persona afectada por una información dar su propia versión de los hechos, aunque en definitiva pudiera revelarse inexacta[622].

En España la protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen se halla regulada por la Ley Orgánica 1/82. Finalmente, el ordenamiento reserva la protección penal para los atentados más graves al honor (delitos de injurias y calumnias) y a la intimidad (diversos tipos delictivos que sancionan hechos contrarios a este bien, como la revelación de secretos, el allanamiento de morada y otros).

La pluralidad en las vías de protección es necesaria puesto que, el principal factor que origina esta conveniencia, es el que una persona ha de poder elegir el alcance de la satisfacción que pretende, puesto que en algunos casos la publicidad del asunto puede ocasionar más perjuicios al proyectar la atención por parte de los medios de prensa e Internet[623].

---

[622] STC 168/1986, de 22 de diciembre.

[623] *Vid. Infra* Cap. V.5.2 sobre el efecto Streisand.

El procedimiento de oposición, acceso, rectificación o cancelación según el artículo 17 de la LOPD está definido de forma reglamentaria y también, no se podrá exigir contraprestación alguna por el ejercicio de estos derechos.

En lo que respecta a la tutela de estos derechos, el titular afectado podrá acudir ante la AEPD cuando se haya dispuesto en contra de los derechos contenidos en la LOPD, entre los que se incluyen los derechos de oposición, acceso, rectificación o cancelación[624].

Es importante señalar que en la Ley costarricense que regula los aspectos de la protección de datos personales, no se incluye el derecho de indemnización, el cual resulta necesario se disponga tal y como se hace en la LOPD, específicamente, en el artículo 19, al establecer que, el incumplimiento de lo dispuesto en esa Ley por el responsable o el encargado del tratamiento, que provoque un daño o lesión al interesado en sus bienes o derechos tendrá que indemnizarlo.

Para los asuntos tramitados en Costa Rica, se deberá acudir a los mecanismos ordinarios de indemnización que dispone el ordenamiento civil, en caso de particulares o en caso de que se trate de una infracción cometida por parte de las autoridades públicas ante la Jurisdicción Contenciosa Administrativa.

---

[624] *Vid.* Art. 18 de la LOPD.

3.3. En Costa Rica.

3.3.1. Derecho de acceso a los datos personales.

La jurisprudencia de la Sala Constitucional de Costa Rica ya tutelaba este derecho desde antes de la aprobación de la Ley No. 8968, Ley de protección de la persona frente al tratamiento de sus datos personales, así la SSC 1345-1998 inicia con una noción básica del derecho a la intimidad, señalando que era insuficiente dicha protección ante los peligros que presenta la sociedad de la información, aunque todavía no reconoce la existencia del derecho a la autodeterminación informativa.

Posteriormente, en la SSC 04847-1999 se desarrolló por primera vez este concepto, reconociendo el derecho a la autodeterminación informativa, como una derivación del derecho a la intimidad, ante el desarrollo de nuevas tecnologías que facilitan el transporte de información y también se reconoció, al lado de este, el derecho a estar informado del procesamiento de los datos y de los fines que con él se pretende alcanzar, junto con el derecho de acceso, corrección o eliminación en caso el que se le cause un perjuicio ilegítimo.

Antes de la entrada en vigencia de la Ley No. 8968, el derecho de acceso a los datos personales fue delimitado por la jurisprudencia de la Sala Constitucional, reconocido como el derecho que permite el acceso al titular cuando se encuentra registrado de alguna forma en un banco o base de datos, es decir, el derecho a saber lo que en él consta acerca de su persona[625].

[625] *Vid.* SSC 05802-99 de las 15:36 hrs. del 27 de julio de 1999.

Esta es la típica tutela del derecho a la información, a partir de la cual el sujeto puede accionar con el fin de ejercer control de los datos que sobre él se encuentran registrados. Además, se reconoce que este derecho puede descomponerse en dos momentos, el primer en el cual se manifiesta el derecho de conocer los datos personales que constan en el registro y, el segundo como derecho de acceso en el cual se toma conocimiento del contenido de la información existente[626].

Entre los derechos reconocidos en la Ley No. 8968[627], se reconoce en el artículo 7.1 el derecho de acceso a la información, garantizando el derecho de acceso por la persona interesada a la información almacenada. Varias facultades se introducen en esa normativa, tales como:

a) Obtener en intervalos razonables, según se disponga por reglamento, sin demora y a título gratuito, la confirmación o no de la existencia de datos suyos en archivos o bases de datos. En caso de que existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.

b) Recibir 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.

c) Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes a terceros, aun cuando se vinculen

---

[626] *Vid.* SSC 05802-99 de las 15:36 hrs. del 27 de julio de 1999.

[627] *Vid.* Art. 7.1 de la Ley No. 8968, Ley de protección de la persona frente al tratamiento de sus datos personales.

con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.

d) Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales.

Así mismo, se determinó que el acceso a la información podía ser ejercido, en el caso de personas fallecidas, por parte de sus herederos o sucesores.

3.3.2. Derechos rectificación, cancelación, oposición y olvido o supresión.

En el contexto latinoamericano se han protegido los derechos de las personas frente al tratamiento de sus datos personales a través del recurso de hábeas data. En ese sentido, lo apunta Chirino Sánchez[628], al afirmar que este acercamiento al tema, a través del recurso de hábeas data, ha provocado que el desarrollo normativo haya comenzado con prever las garantías a la tutela jurisdiccional[629] antes que se reconociera como un verdadero derecho fundamental en los textos normativos.

De esta manera el recurso de hábeas data se convierte en Latinoamérica en una garantía o mecanismo jurídico procesal que actúa como instrumento para la defensa del derecho a la intimidad y la protección de datos personales al garantizar

---

[628] CHIRINO SÁNCHEZ, A., "La Ley de Protección de Datos de Costa Rica. Luces en las sombras", op. cit., p. 9.

[629] Es en la SSC 04847-99 de las 16:27 hrs. del 22 de junio de 1999, que desarrolla por primera vez el derecho a la autodeterminación informativa, como un derecho derivado del derecho de intimidad. En esta sentencia se reconoce el derecho a estar informado del procesamiento de los datos y de los fines que con él se pretende alcanzar, junto con el derecho de acceso, corrección o eliminación en caso el que se le cause un perjuicio ilegítimo.

el acceso, la rectificación y cancelación de los datos de las personas contra el uso indebido por parte de otras.

La Ley de la Jurisdicción Constitucional de Costa Rica no contempló el proceso de hábeas data, sin embargo, este proceso fue reconocido en los primeros fallos luego de creada la Jurisdicción Constitucional en 1989. Así el recurso de hábeas data se tramitó como una especia de recurso de amparo "especial" mediante el cual se tutelan los derechos relacionados con la intimidad y la protección de datos personales, entre los que se incluyeron los derechos de acceso, corrección o eliminación de los datos. Ante la falta de una regulación específica, la Sala Constitucional mantuvo el criterio de protección a través del recurso de amparo.[630]

Si bien la defensa del derecho a la intimidad y la autodeterminación informativa encontraron en el contexto de la región un mecanismo jurídico a la protección, lo cierto es que a través de ese recurso se tutelan los derechos

---

[630] Debe advertirse que luego de la aprobación y vigencia de la Ley de protección de la persona frente al tratamiento de sus datos personales, la Sala Constitucional, declinó la tutela de los datos personales en la Agencia de Protección de Datos Prodhab, la cual entró en funciones el 5 de marzo de 2012. A partir de la SSC 2013-013326 de las 9:05 hrs. del 4 de octubre de 2013, se indicó: "*II.- NUEVO MECANISMO PARA LA PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES. Las sentencias de este Tribunal han desarrollado ampliamente el derecho al olvido y por la vía del amparo se han conocido y resuelto vulneraciones al tratamiento de datos personales. Sin embargo, esta materia ya no procede ser dilucidada por este Tribunal constitucional, por cuanto la Ley 8968 o Ley de Protección de la Persona frente al tratamiento de sus datos personales, creó un órgano y un procedimiento especializados, para investigar lo que la parte recurrente reclama en su escrito de interposición del recurso. (…) De conformidad con lo expuesto, es ante la Agencia de Protección de Datos de los habitantes (Prodhab) donde la parte recurrente podrá dirigir -si a bien lo tiene- sus reclamos con respecto a la alegada lesión del derecho a la cancelación de sus datos (que a su vez forma parte del derecho a la autodeterminación informativa), máxime que no se tiene por acreditado que la persona amparada haya presentado gestión alguna ante esa autoridad con el fin de que se cancelen sus datos personales en los registros que tiene en su poder el sujeto de derecho privado recurrido. La Agencia de Protección de Datos (Prodhab) entró en funciones el 5 de marzo de 2012 y a ella compete tramitar y resolver el asunto en sede administrativa, sin perjuicio de las garantías jurisdiccionales que en derecho corresponden. Así las cosas, el presente recurso es inadmisible y así se declara*".

señalados cuando la lesión se ha producido, de manera que, la jurisdicción constitucional se limita a la reivindicación o indemnización de los derechos tutelados.

Dado el reconocimiento jurisprudencia de la Sala Constitucional sobre el recurso de hábeas data, como mecanismo para la protección de los datos de las personas, se desarrolló, en ese momento y, con anterioridad a la aprobación de la ley especial, una serie de objetivos que ampliaban la protección del derecho a la intimidad y del derecho a la protección de los datos personales de la siguiente manera[631]:

*"**a) Derecho al acceso:** cuando un sujeto se encuentra registrado en alguna forma en un banco o base de datos, tiene derecho a saber lo que en él consta acerca de su persona. Es la típica tutela del derecho a la información, a partir de la cual el sujeto puede accionar con el fin de ejercer control sobre los datos que sobre él se encuentran registrados. Este derecho puede descomponerse en dos momentos, uno en el que se manifiesta el derecho de conocer los datos personales que constan en el registro y un derecho de acceso en el que se toma conocimiento del contenido de la información existente.*

***b) Derecho a la actualización:** permite que los datos relativos a ella sean exactos, de manera que evita la consignación de datos falsos acerca de la persona registrada. Junto con este derecho se debe incluir, lógicamente, el derecho a la rectificación del dato registrado.*

***c) Derecho a la confidencialidad:** a través suyo 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*

---

[631] *Vid.* SSC 05802-99 de las 15:36 hrs. del 27 de julio de 1999.

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.

d) Derecho a la exclusión: *se refiere a la recolección de la denominada información sensible, de manera que por medio del hábeas data la persona puede solicitar la cancelación de los datos consignados y evitar así los eventuales tratos discriminatorios por parte de las personas que tengan acceso a ella. El sujeto puede solicitar la cancelación del dato registrado cuando su recolección ha sido prohibida, cuando sea impertinente para la finalidad perseguida por la base de datos o en el supuesto de que, por el transcurso de tiempo, no resulte necesario mantener el dato en el registro.*

e) Derecho de inserción: *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.*

f) Derecho a saber del conocimiento de terceros sobre la información recolectada: *es el derecho de saber qué información relativa al sujeto ha sido facilitada a terceros: a quién ha sido facilitada y para qué efectos."*

Con base en estos elementos señalados, la Sala Constitucional define el recurso de hábeas data, "*como el mecanismo procesal que tiende a garantizar a todo sujeto la posibilidad de acceder a los bancos de datos -públicos o privados-, tomar conocimiento de la información referida a su persona, corregir la que fuere distorsionada o hacer cancelar la que no fuera pertinente con la finalidad para la cual fue obtenida y en términos más generales, tiende a oponer la libertad del sujeto al avance de la tecnología en el campo de la información y la comunicación y a la protección de un ámbito de intimidad en el cual el sujeto tiene derecho a desenvolverse. Se trata de un viraje en la forma de concebir el hábeas data donde*

al sujeto se le da la posibilidad de acceder a la información, verificar su contenido, exigir la corrección o cancelación de los datos recolectados de forma que se haga transparente la circulación de la información legalmente registrada"[632].

La citada sentencia también hace un aporte importante al indicar la necesidad de transparencia en todas las etapas del procesamiento de datos personal y al delimitar las posibilidades de intervención de los usuarios, para que los ciudadanos puedan ejercer un adecuado control de sus datos personales[633].

Asimismo, señala el Tribunal Constitucional que el recurso de hábeas corpus no puede ser considerado como un mecanismo para atacar los archivos de información en general, ni pretende la eliminación de todo tipo de registro o banco de datos, sino que debe ser aplicado en el resguardo de los fines del tratamiento de la información, de la proporcionalidad de uso de las informaciones, de la seguridad, pertenencia y veracidad de los datos recabados, para el resguardo de datos sensibles y para permitir la realización del individuo en la sociedad marcada por el signo tecnológico[634].

Con posterioridad, en el año 2012, se aprobó el primer instrumento jurídico en materia de protección de datos personales en Costa Rica, la Ley No. 8968[635], Ley de protección de la persona frente al tratamiento de sus datos personales, y ha llenado un vacío normativo, de tal manera que complementa el trabajo realizado por

---

[632] *Vid.* SSC 05802-99 de las 15:36 hrs. del 27 de julio de 1999.

[633] *Ibid.*

[634] *Ibid.*

[635] La Ley No. 8968 fue tramitada bajo el expediente legislativo número 16679, que fue presentado en la Asamblea Legislativa el 19 de junio de 2007 y, finalmente vigente como ley de la República desde el 5 de setiembre de 2011.

parte de la Jurisdicción Constitucional al permitir el control y organización del tratamiento de datos personales en Costa Rica. A partir de la aprobación la citada Ley, se incorporan al ordenamiento jurídico costarricense los mecanismos, para que, de forma previa se garantice el procesamiento de datos.

Esta Ley está ordenada en 6 capítulos con un total de 34 artículos. En el artículo 7 se señalan los derechos que asisten a las personas, en el inciso 1 el derecho de acceso a la información[636] y en el inciso 2 el derecho de rectificación.

En lo que respecta al derecho de rectificación se dispone en el artículo 7.2 de la Ley No. 8968 lo siguiente:

"Se garantiza el derecho de obtener, llegado el caso, la rectificación de los datos personales y su actualización o la eliminación de estos cuando se hayan tratado con infracción a las disposiciones de la presente ley, en particular a causa del carácter incompleto o inexacto de los datos, o hayan sido recopilados sin autorización del titular.

Todo titular puede solicitar y obtener de la persona responsable de la base de datos, la rectificación, la actualización, la cancelación o la eliminación y el cumplimiento de la garantía de confidencialidad respecto de sus datos personales.

El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, le corresponderá a sus sucesores o herederos."

En la citada normativa, bajo el título del derecho de rectificación, se han reconocido los derechos relacionados con la rectificación, la actualización, la cancelación o la eliminación y el cumplimiento de la garantía de confidencialidad,

[636] Vid. *Supra* Cap. V. 4.3.1.

es decir, se han agrupado a efectos normativos y no se señalan otras consideraciones adicionales a efectos de la protección de estos derechos.

Ha de advertirse que el procedimiento por medio del cual se ejercitan los derechos de acceso a la información y el de rectificación son gratuitos y deberán ser resueltos en un plazo de cinco días hábiles desde la recepción de la solicitud.

Tratándose del derecho de acceso a la información, la persona se encuentra facultada para obtener la confirmación o no sobre la existencia de datos suyos en archivos o bases de datos, recibir información relativa a su persona, así como la finalidad con que dichos datos fueron recopilados y el uso que se les dará. Adicionalmente, el titular de los datos tendrá el derecho de ser informado por escrito sobre la totalidad del registro de los datos relacionados con su persona. Aun cuando el requerimiento solo comprenda un aspecto de los datos personales, tendrá derecho a que se le informe sobre el programa, el método o el proceso utilizado en los tratamientos de sus datos personales.

Asimismo, sobre el derecho de rectificación, el titular de los datos tiene el derecho de solicitar la rectificación, actualización o eliminación de sus datos personales, que hubiesen sido tratados con infracción a las disposiciones de esa ley. Este derecho, al igual que el de información, también podrá ser ejercicio por los herederos del titular.

Es importante recalcar que, aunque el legislador haya incluido en el mismo artículo del derecho de rectificación los derechos de actualización o eliminación debe considerarse que las consecuencias jurídicas del ejercicio de uno u otro derecho son distintas. Mientras que en el ejercicio del derecho a la rectificación lo que se pretende es la corrección por inexactitud de un dato de la persona, tratándose del derecho de cancelación o eliminación la consecuencia sería la supresión del dato, situación que podría justificarse por una falta en el consentimiento, por tratase de datos sensible, por la actualidad de los datos o porque la persona ha revocado el consentimiento.

A través del Decreto Ejecutivo No. 37554 del 30 de octubre de 2012, se aprobó el Reglamento a la Ley de Protección de la persona frente al tratamiento de sus datos personales, el cual se encuentra vigente desde el 5 de marzo de 2013. En esta reglamentación se indicó en el artículo 13 que el ejercicio de los derechos de acceso, de rectificación, de modificación, de revocación o de eliminación de los datos personales, no excluye la posibilidad de ejercer unos u otros, ni puede constituir requisito previo para el ejercicio de cualquiera de estos derechos.

Las restricciones[637] para el ejercicio de estos derechos sólo podrán fundamentarse en cuestiones de seguridad nacional, disposiciones de orden público y salud pública o para proteger los derechos de terceras personas, en los casos y con los alcances previstos en las leyes aplicables en la materia, mediante resolución de la autoridad competente debidamente fundamentada y motivada[638].

La legitimación para el ejercicio de los derechos de acceso, rectificación, modificación, revocación o eliminación se dispuso en el artículo 15 de la normativa citada y para ello el titular o representante de los datos deberá acreditarse de forma previa.

El derecho de rectificación está limitado según se dispone en el artículo 23 de forma tal que el titular o su representante podrá rectificar los daros que resulten ser inexactos, incompletos o confusos.

El artículo 24 del citado reglamento, señala que las solicitudes de rectificación de los datos deberán contener los siguientes requisitos:

---

[637] Vid. Art. 14 del Decreto Ejecutivo No. 37554 del 30 de octubre de 2012, Reglamento a la Ley de Protección de la persona frente al tratamiento de sus datos personales.

[638] Sobre los límites del derecho a la autodeterminación informativa puede consultarse *supra* en el Cap. V.3.3.

- Indicar a qué datos personales se refiere la solicitud de rectificación o eliminación.
- Indicar la corrección que se solicita realizar, y
- Aportar la documentación o prueba pertinente que ampare la procedencia de lo solicitado.

En cuanto al derecho de supresión o eliminación de los datos, el reglamento señala en el artículo 25 que el titular podrá solicitar en cualquier momento al responsable, la supresión o eliminación total o parcial de los datos personales del titular, de manera definitiva.

En el artículo 26 se indican las excepciones para el ejercicio del derecho de supresión o eliminación de los datos, en el cual se disponen los siguientes:

a) La seguridad del Estado,

b) Los datos deban ser mantenidos por disposición constitucional, legal o resolución de órgano judicial,

c) La seguridad ciudadana y el ejercicio de la autoridad pública,

d) La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones deontológicas de los profesionales,

e) El funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas,

f) La adecuada prestación de servicios públicos,

g) La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales y,

h) Se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general.

Debe advertirse que, uno de los problemas comunes e identificados respecto al tratamiento de datos personales se refiere a la falta de conocimiento de las personas sobre los derechos relacionados con el procesamiento y almacenamiento de sus datos personales. Pareciera necesario que se realizasen campañas para informar a la población sobre los derechos que les asisten y la forma de ejercitarlos de forma adecuada.

E lo que respecta a las excepciones se omite en la regulación la forma de aplicarlas, pareciera necesario que en el texto se hubiese obligado a que en los casos de excepción se realice mediante una resolución fundada, además de la obligación de valorar la excepción ante principios los principios de necesidad, razonabilidad y proporcionalidad.

4. EXCEPCIONES AL DERECHO DE PROTECCIÓN DE DATOS.

Como la mayoría de los derechos fundamentales, la protección de datos personales no es considerado como absoluto y tienes límites, siempre que tales limitaciones estén establecidas por la ley, respeten el contenido esencial de dichos derechos y libertades y, cumpliendo el principio de proporcionalidad, sean necesarias y respondan, efectivamente, a objetivos de interés general.

En Europa el derecho a la protección de los datos de carácter personal está protegido en el artículo 8 de la Carta de los Derechos Fundamentales, en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) y en el artículo 8 del CEDH. Como subrayó el Tribunal de Justicia de la UE[639], el derecho a la protección de datos de carácter personal no es un derecho absoluto, sino que se ha de considerar en relación con su función en la sociedad. En ese sentido, señaló que "*…el artículo 52, apartado 1, de la Carta reconoce que pueden introducirse limitaciones al ejercicio de derechos como los consagrados de los artículos 7 y 8 de la misma, siempre que tales limitaciones estén establecidas por la ley, respeten el contenido esencial de dichos derechos y libertades y, respetando el principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás* [Estados]".

La mayoría de excepciones que pueden observarse en las normas relacionadas con la protección de datos personales, están fundamentadas en el

[639] *Vid.* Sentencia del Tribunal de Justicia de la UE (Gran Sala), de 9 de noviembre de 2010, en los asuntos acumulados, Volker und Markus Schecke C-92/09 y Hartmut Eifert Land Hessen C-93/09, [en línea], http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=152652

interés común frente al interés individual, como por ejemplo lo sería el defensa del Estado, la seguridad nacional, la protección de derechos y libertades de terceros o la persecución de infracciones penales o administrativas.

4.1. En los Estados Unidos de América.

Según Paul M. Schwartz[640], el acceso a la información personal y la fijación de sus límites coadyuva a la conformación de la sociedad y a la definición de la identidad personal, por cuanto la estructura de acceso a la información personal ejerce un impacto decisivo en la medida en que son fomentadas ciertas acciones o expresiones de la identidad individual. De esta manera, la importancia de la reserva de la información personal tanto para el individuo como para la sociedad, requiere la determinación de los límites del ámbito protegido de la información personal, de ahí que la "privacidad constitutiva" exija la delimitación normativa de los niveles estandarizados de escrutinio. Así, Schwartz defiende una regulación estatal generalizada, que asegure el control efectivo sobre el flujo de información personal, propone así un modelo estatal que interviene en el ámbito de la información individual, por ser este uno de los valores esenciales de los nuevos paradigmas sociológicos de principios del siglo XXI.

Tal y como se señaló en el capítulo III *supra* existen en los EE.UU. numerosas disposiciones normativas con el objeto de regular sobre la privacidad de la vida íntima de las personas, sin embargo, también se han dispuesto una gran cantidad de reformas que permiten el acceso a información de las personas como excepción, tales como el *Bank Secrecy Act (BSA) of* 1970[641], el *Communications Assistance for Law Enforcement Act (CALEA) of* 1994[642], el *Personal Responsibility and Work*

---

[640] SOLOVE, D. J. y SCHWARTZ P. M., *Privacy, information and technology*, *op. cit.*, pp. 57-59; SCHWARTZ P. M., "Privacy and Democracy in Cyberspace", *op. cit.*, pp. 1609 y ss.

[641] Bank Secrecy Act (BSA) of 1970, Pub. L. 91–508, [en línea], https://www.law.cornell.edu/uscode/text/31/5311

[642] Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. 103–414, [en línea], https://www.law.cornell.edu/uscode/text/18/2522

Opportunity Reconciliation Act (PRWOR) of 1996[643], y el *USA-PATRIOT Act of* 2001[644].

Se muestra como en las últimas décadas, el Congreso de los EE.UU., ha dispuesto una serie de leyes con el propósito de regular las eventuales intromisiones a la vida privada de las personas y los datos de estas y, de otra parte, también se muestran las limitaciones y excepciones relacionadas con la posibilidad de disponer de esta protección.

En ese sentido Daniel Solove[645] plantea el *argumento del péndulo,* mediante el cual explica que en tiempos de crisis se deben sacrificar las libertades civiles y los derechos constitucionales para conseguir más seguridad. Una vez que se supera el período de crisis son restaurados los derechos que fueron suspendidos[646].

---

[643] Personal Responsibility and Work Opportunity Reconciliation Act (PRWOR) of 1996, Pub. L. 104–193, [en línea], http://www.law.cornell.edu/uscode/text/42/616&prev=search

[644] USA-PATRIOT Act of 2001, Pub. L. No. 107-56, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[645] SOLOVE, D. J., *Nothing to hide: the false tradeoff between privacy and security,* Yale University Press, New Haven and London, 2013, pp. 55-61.

[646] Indica SOLOVE. "*Me refiero a este argumento como el "argumento de péndulo" - en tiempos de crisis, el péndulo oscila hacia seguridad y los derechos se reducen, y en tiempos de la paz, el péndulo oscila de nuevo hacia la libertad y la se restauran los derechos. Pero el argumento de péndulo debe entenderse al revés, pues en los tiempos de crisis, precisamente, es cuando debe estar más firme nuestra protección de la privacidad y la libertad*". SOLOVE, D. J., *Nothing to hide: the false tradeoff between privacy and security, op. cit.,* pp. 55-56.

4.2. En Europa y España.

La Directiva 95/46/CE relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos de 24 de octubre de 1995, contempla excepciones al derecho a la protección de datos personales. En el considerando 33 se señala el consentimiento como primera excepción al tratamiento de datos personales, en lo que interesa indica que "*…los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su* ***consentimiento explícito****; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con* ***fines relacionados con la salud****, por parte de personas físicas sometidas a una* ***obligación legal de secreto profesional****, o para* ***actividades legítimas*** *por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales"*[647]*.* En el mismo sentido ver el considerando 58 de la citada directiva.

En igual sentido, el considerando 34 autoriza a los *"…Estados miembros, cuando esté justificado por razones de interés público importante, a hacer* ***excepciones a la prohibición*** *de tratar categorías sensibles de datos en sectores como la* ***salud pública*** *y la* ***protección social****, particularmente en lo relativo a la* ***garantía de la calidad y la rentabilidad****, así como los procedimientos utilizados para* ***resolver las reclamaciones de prestaciones*** *y de* ***servicios en el régimen***

[647] *Vid.* Considerando 33 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre del 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

***del seguro enfermedad**, la **investigación científica** y las **estadísticas públicas**; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas"*[648].

De igual forma, normativa marco se expone la necesitad de prever excepciones o restricciones de determinadas disposiciones en caso de ser necesarias para conciliar los derechos fundamentales de las personas con la libertad de expresión y, en particular, con la libertad de expresión, para recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales[649].

También se prevé, en la citada normativa comunitaria[650], la posibilidad de imponer límites al derecho de acceso a la información pública, cuando resulten necesarios para salvaguardar la seguridad del Estado, la defensa, la seguridad pública, los intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como para realizar investigaciones y entablar procedimientos penales y perseguir violaciones de normas deontológicas en las profesiones reguladas; señala además, que deben enumerarse, a efectos de excepciones y limitaciones, las tareas de control, inspección o reglamentación necesarias en los tres últimos sectores mencionados relativos a la seguridad pública, los intereses económicos o financieros y la represión penal; y que esta enumeración de tareas

---

[648] *Vid.* Considerando 34 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

[649] *Vid.* Considerando 37 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

[650] *Vid.* Considerando 43 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

relativas a los tres sectores citados no afecta a la legitimidad de las excepciones y restricciones establecidas por razones de seguridad del Estado o de defensa.

Siempre que se dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público, establecer otras excepciones[651]. En la sección VI, se incluyeron en el artículo 13 las excepciones y limitaciones:

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones deontológicas en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); y

g) la protección del interesado o de los derechos y libertades de otras personas.

---

[651] *Vid.* Art. 8.4 y 8.5 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que de forma manifiesta no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12, cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal, durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas[652].

De forma mejorada en la nueva Propuesta[653] del Reglamento General de Protección de Datos UE, se señalan excepciones a la prohibición de tratar categorías sensibles de datos, siempre que se haga mediante un acto legislativo y se den las garantías apropiadas, a fin de proteger los datos personales y otros derechos fundamentales, cuando así lo justifiquen razones de interés público, incluidas la sanidad pública, la protección social y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o para fines de investigación histórica, estadística y científica.

En el artículo 21[654], se establecen las limitaciones al tratamiento de los datos personales, siempre y cuando tal limitación constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar:

---

[652] *Vid.* Art. 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

[653] Considerando 42 de la Propuesta del Reglamento General de Protección de Datos de la U.E., [en línea], http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=es.

[654] *Vid.* Art. 21 de la Propuesta del Reglamento General de Protección de Datos de la U.E..

a) la seguridad pública;

b) la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales;

c) otros intereses públicos de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, especialmente en los ámbitos fiscal, presupuestario y monetario, así como la protección de la estabilidad y la integridad de los mercados;

d) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

e) una función reglamentaria, de inspección o de supervisión relacionada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a), b), c) y d); y

f) la protección del interesado o de los derechos y libertades de otras personas.

A partir del Capítulo IX del citado reglamento[655], se desarrollan las reglas relativas a situaciones de tratamiento de datos específicas, en las cuales se prevén excepciones para cada una de esas situaciones. Estas disposiciones específicas están relacionadas con: el tratamiento de datos personales y libertad de expresión, el tratamiento de datos personales relativos a la salud, el tratamiento en el ámbito laboral, el tratamiento para fines de investigación histórica, estadística o científica,

[655] *Vid.* Arts. 80-85 Art. 21 de la Propuesta del Reglamento General de Protección de Datos de la U.E..

las obligaciones de secreto y las normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.

Se podría inferir que la especialidad lograda en esta propuesta podría responder a la fragmentación legislativa de la protección de datos de carácter personal en la UE[656], la inseguridad jurídica y la percepción generalizada de la opinión pública[657], al estimar que existen riesgos significativos, en especial por lo que se refiere a la actividad en línea. Por ello se percibe un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación más estricta, lo que parece permitirá el desarrollo de la economía digital en el mercado interior, otorgando a los ciudadanos control mejorado de sus propios datos y reforzando la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas.

En la LOPD no se observa un apartado dedicado a las excepciones o límites relativo al tratamiento de los datos personales, como se implementa en la normativa general de la UE. En la LOPD se ha dispuesto que en el reglamento se determinará

---

[656] Sin el ánimo de que se adelanten conclusiones, en lo particular, el autor estima que el marco jurídico actual de la UE es uno de los mejores modelos en materia de protección de datos personales y como cualquier modelo es susceptible de mejoras y ajustes, para lo cual deberán realizarse constantes exámenes y revisiones de forma permanente y sistemática, lo anterior en razón del constante crecimiento del tratamiento de datos de forma electrónica.

[657] Según los resultados mostrados por el Eurobarómetro (de 24 d junio de 2015) la protección de los datos personales sigue siendo una preocupación importante para los ciudadanos. El hallazgo central de la encuesta muestra que la confianza en entornos digitales sigue siendo baja. Dos tercios de los encuestados (67%) dicen que están preocupados por no tener control sobre la información que proporcionan en línea, mientras que sólo el 15% sienten que tienen el control completo, seis de cada diez encuestados manifestaron su desconfianza en los negocios en línea (63%), y en las empresas de telefonía y proveedores de servicios de Internet (62%), [en línea], http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm

un procedimiento[658] por medio del cual, por excepción, y atendiendo a los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se pueden mantener determinados datos.

En primer lugar, se tiene la excepción de protección para los datos personales de acceso público[659], la cual se refiere a los ficheros cuya consulta puede ser realizada por cualquier persona siempre que no esté impedida por una norma limitativa y sin más exigencia que, en su caso, el abono de una contraprestación.

En segundo lugar, en el artículo 23[660] se prevén excepciones relacionadas con el acceso, la rectificación o cancelación de datos personales, en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Finalmente, en el artículo 24.1[661] se prevén otras excepciones relacionadas a la recogida de datos cunado la información impida o dificulte, gravemente, el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

---

[658] *Vid.* Art. 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) (BOE núm. 298, de 14-12-1999, pp. 43088-43099). Consultable en: http://civil.udg.es/normacivil/estatal/persona/PF/lo15-99.htm.

[659] *Vid.* Art. 3. J) de la LOPD y art. 7 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado mediante Real Decreto 1720/2007.

[660] *Vid.* Art. 23 de la LOPD.

[661] *Vid.* Art. 24.1 de la LOPD.

Debe recordarse que mediante STC 292/2000 de 30 de noviembre de 2000. Se resolvió el recurso de inconstitucionalidad número 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Persona, en el que argumentó la vulneración del derecho fundamental a la protección de datos personales, sentencia en el cual se dispuso la inconstitucionalidad parcial de los artículos 21.1 y 24.1 y la totalidad del artículo 24.2, todos de la LOPD, al estimarse contrarios al derecho de la Constitución.

4.3. En Costa Rica.

El 7 de julio de 2011 se aprobó la Ley No. 8968, Ley de protección de la persona frente al tratamiento de sus datos personales, que entró en vigencia el 5 de setiembre de 2011 y por medio de la cual se creó la Agencia de Protección de Datos Personales (Prodhab), órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz. Esta constituye la norma principal para la protección de los datos personales en Costa Rica, luego de lo preceptuado en el artículo 24 de la Constitución Política, sin embargo también se incluyeron una serie de excepciones a la protección de datos personales, limitación que deberá realizarse de manera justa, razonable y acorde con el principio de transparencia administrativa cuando se persigan los siguientes fines[662]:

a) La seguridad del Estado.

b) La seguridad y el ejercicio de la autoridad pública.

c) La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones deontológicas en las profesiones.

d) El funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas.

e) La adecuada prestación de servicios públicos.

f) La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

---

[662] Art. 8 “Excepciones a la autodeterminación informativa del ciudadano”, Ley No. 8968, Ley de protección de la persona frente al tratamiento de sus datos personales.

En esta normativa se establecen las condiciones para limitar las garantías establecidas con respecto al derecho de la autodeterminación informativa. En este sentido no se indica que ello requiera una resolución fundada, razonamiento que se estima necesario a efecto de advertir al titular de los datos, las razones por las cuales se niega una solicitud de protección o se utilizan sus datos sin requerir su consentimiento de forma previa, lo anterior para que pueda tomar las medidas que estime necesarias en caso de no estar conforme con las medidas acordadas.

Según apunta Chirino Sánchez, el legislador pretendió, con la aprobación de la citada normativa, imponer límites al derecho de autodeterminación informativa y definió que, la seguridad del Estado, la prevención y persecución de los delitos serían objetivos que no podrían limitarse con el argumento de proteger esta garantía. Sin embargo, considera que tales excepciones deberían de pasar por el tamiz de principios tales como el de justicia, razonabilidad y transparencia administrativa, a los que habría que agregar el de proporcionalidad[663].

En ese sentido, para Chirino Sánchez, "*no sería posible pensar ninguna limitación de este derecho si no se ha realizado un análisis de su necesidad, adecuación e idoneidad para cumplir el fin público del que se trate. Aun después de este análisis, habría que preguntarse si la limitación es "soportable" individualmente para el sujeto que la sufre en razón de esos fines públicos que se plantea realizar*"[664].

---

[663] CHIRINO SÁNCHEZ, A., "La Ley de Protección de Datos de Costa Rica. Luces en las sombras" en *Revista Internacional de Protección de Datos Personales*, Universidad de los Andes. Facultad de Derecho, No. 1 julio - diciembre de 2012, p. 7.

[664] CHIRINO SÁNCHEZ, A., "La Ley de Protección de Datos de Costa Rica. Luces en las sombras", *op. cit.,* pp.7-8.

Adicionalmente, debe señalarse que en la mayoría de legislaciones se desprotege la información cuando los datos recolectados no están asociados a las personas[665], sin embargo, se estima conveniente se replanteen esas disposiciones en razón de la posibilidad de que las informaciones relacionadas con las personas, aunque sean despersonalizadas, numeradas o anónimas, corren un alto riesgo de que el titular pueda ser identificado. En otros apartados de esta investigación ya se han advertido estas razones y se han expuesto casos, como la posibilidad de que programas de computadoras identifiquen a la persona apenas con algunos de los supuestos datos despersonalizados, así como la creación de perfiles y patrones, y, la creciente actividad de los corredores de datos (*data brokers)* quienes elaboran perfiles de información de las personas con fines comerciales.

[665] *Vid.* Art. 8 inciso d) de la Ley No. 8968, Ley de protección de la persona frente al tratamiento de sus datos personales.

5. DERECHO AL OLVIDO EN INTERNET.

En 1785 el Rey Carlos III ordenó que toda la documentación referida a los dominios españoles en las Indias, fuese trasladada a la Real Casa de la Lonja de Mercaderes de Sevilla. Documentos que se encontraban en los archivos del Consejo de Indias de Madrid, Central de Simancas en Valladolid y la Casa de Contratación de Cádiz y de Sevilla, fueron trasladados para crear el Archivo General de Indias.

Este archivo cuenta con casi 43.000 legajos, 80 millones de páginas y 8.000 mapas y dibujos que juntos ocupan más de nueve kilómetros, siendo considerado como el mayor archivo de la actividad de España en América y Filipinas. En este se resguarda la historia política, social y económica de la época. Siendo un recordatorio de la importancia y el costo que ha tenido el resguardo de la información para los seres humanos.

En la actualidad el costo de guardar, transmitir y proteger la información ha cambiado considerablemente y no se compara con los esfuerzos del Archivo de Indias. Las tecnologías, y principalmente, Internet, se han encargado de acortar las barreras de espacio y tiempo, aportando, de forma positiva, el disfrute y efectividad de los derechos fundamentales por parte de la sociedad. La gran cantidad de información contenida en servidores en todo el mundo, es alcanzable a través de motores de búsqueda en Internet, los cuales facilitan la localización de los contenidos o información. Estos buscadores han logrado un protagonismo sin precedentes, convirtiendo a las empresas en gigantes de TI. De igual forma, la capacidad de esos motores de búsqueda ha perjudicado la intimidad de las personas, especialmente, en lo relativo al tratamiento de sus datos personales.

Los resultados que muestran los motores de búsqueda han despertado la discusión sobre el roce entre derechos fundamentales, principalmente, entre la libertad de expresión frente al derecho de intimidad y la protección de datos personales, lo cual a ha requerido el pronunciamiento de las más altas autoridades

judiciales europeas. En el conocido caso de Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, de 13 de mayo de 2014[666], se sienta un gran precedente sobre el derecho al olvido en Internet, al calificar la actividad de los motores de búsqueda en Internet como tratamiento de datos personales y sentando las responsabilidades del caso por el tratamiento de esos datos.

El derecho al olvido referido no es más que la aplicación en Internet de los derechos de oposición y cancelación, una cuestión que ha suscitado hasta ahora cierta controversia. En el apartado anterior, se analizó la propuesta de Reglamento de protección de datos personales que, de manera expresa, plantea el derecho al olvido en Internet, reconociendo al interesado este derecho para que el responsable suprima los datos personales que le conciernan y se abstenga de seguir utilizándolos y, principalmente, de no continuar con la publicidad de estos, en el entendido que los datos ya no sean necesarios en relación con los fines, haya expirado el plazo de conservación autorizado, se haya cumplido el periodo de almacenamiento de datos o que el interesado retire el consentimiento o se oponga al tratamiento[667].

Si bien no se encuentra en la doctrina un concepto desarrollado sobre el derecho al olvido, esto no supone un gran problema para la aplicación. El problema

---

[666] Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, Petición de decisión prejudicial: Audiencia Nacional – España, [en línea], http://curia.europa.eu/juris/liste.jsf?num=C-131/12

[667] *Cfr.* Art. 17 de la Propuesta del Reglamento General de Protección de Datos de la U.E..

para la aplicación parece ser de índole técnico y no de índole conceptual[668]. De otra parte, en el derecho anglosajón, el *right to be forgotten* o *right to oblivion*, no ha sido amparado en los textos legales, sin embargo, en los textos doctrinales se trata como un nuevo derecho de la privacidad creado en Europa[669].

En EE.UU. la tendencia ha sido la de proteger el derecho a la libertad de expresión en relación a los motores de búsqueda de Internet. De esta manera lo resolvió la Corte de San Francisco EE.UU., dando la razón al Google al ampararle con la primera enmienda (libertad de expresión) al autorizarlo a manipular los resultados de las búsquedas, al indicar que la puede organizar como mejor le convenga[670].

---

[668] ABRIL, P. S., y PIZARRO MORENO, E., "La intimidad europea frente a la privacidad americana. Una visión comparativa del derecho al olvido" en *InDret Revista para el análisis del derecho*, Barcelona, enero 2014, pp.24-25, [en línea], http://derechoaleer.org/media/files/olvido/1031.pdf

[669] ROSEN, J., "The Right to Be Forgotten", en 64 *Stanford Law Review*, 13 de febrero, 2012, [en línea], http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

[670] ROBERTS, J.J., "Google has free speech right in search results, court confirms", *Gigaom Research*, 17 de noviembre de 2014, [en línea], https://gigaom.com/2014/11/17/google-has-free-speech-right-in-search-results-court-confirms/; DANS, E., "Google y la libertad para manipular los resultados de búsqueda", *Blog Enrique Dans*, 18 de noviembre de 2014, [en línea], http://www.enriquedans.com/2014/11/google-y-la-libertad-para-manipular-los-resultados-de-busqueda.html

5.1. Breve exposición del caso Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González.

5.1.1. Litigio principal.

Siendo uno de los casos más emblemáticos de aplicación de derecho al olvido en internet, pareciera necesario hacer una breve referencia de los hechos que llevaron al pronunciamiento, finalmente, del TJUE.

En 19 de enero de 1998, fue publicado en el diario *La Vanguardia* la noticia de la subasta de inmuebles embargados por la Secretaría de Seguridad Social, en la cual figuraba una propiedad del señor Mario Costeja y su esposa. Esa información fue publicada en el diario impreso y luego en el electrónico en el año 2008.

En el año 2010, el Sr. Costeja solicitar al periódico *La Vanguardia* el retiro de la información, pero este se niega argumentando que su publicación es legal. Por tal motivo, sustentado en la libertad de expresión, Costeja presentó ante la AEPD, una reclamación contra este medio y contra Google Spain y Google Inc., en razón de que al introducir su nombre en el motor de búsqueda de Google obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia, del 19 de enero y del 9 de marzo de 1998, respectivamente, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre del Sr. Costeja González. En la reclamación, el afectado solicitó que se exigiese a La Vanguardia eliminar o modificar la publicación para que no apareciesen sus datos personales. Por otro lado, solicitaba que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia. En este sentido, el afectado

afirmaba que el embargo al que se vio sometido en su día estaba totalmente solucionado y resuelto desde hace años y carecía de relevancia actualmente.

En resolución de 30 de julio de 2010, la AEPD desestimó la reclamación en la medida en que se refería a La Vanguardia, al considerar que la publicación que ésta había llevado a cabo estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores. Sin embargo, se estimó la reclamación contra Google Spain y Google Inc., al considerar la AEPD que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información.

Las empresas Google Spain y Google Inc. interpusieron sendos recursos contra dicha resolución ante la Audiencia Nacional, que decidió acumularlos. Se planteó una consulta de prejudicialidad ante el TJUE.

5.1.2. Planteamiento de la Consulta de prejudicialidad.

La consulta planteada por los Magistrados de la Audiencia Nacional se basa en tres temas, desarrollados a través de varias preguntas.

El primer tema planteado se cuestionan si en materia de protección de datos personales es aplicable la normativa de la UE o se debería acudir ante las instancias jurisdiccionales de los EE.UU. domicilio legal de la empresa Google Inc.[671]

[671] Para desarrollar este primer tema formulan las siguientes interrogantes:

El segundo tema planteado se pregunta si los motores de búsqueda que indexan información legítima están obligados a atender los derechos de cancelación, rectificación u oposición frente a las personas titulares de los datos.[672]

1.1. ¿Debe interpretarse que existe un "establecimiento", en los términos descritos en el art. 4.1.a) de la Directiva 95/46/CE, cuando concurra alguno o algunos de los siguientes supuestos: -cuando la empresa proveedora del motor de búsqueda crea en un Estado miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes de ese estado, o -cuando la empresa matriz designa a una filial ubicada en ese estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa o -cuando la oficina o filial establecida en un estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria?.

1.2. ¿Debe interpretarse el art. 4.1.c de la Directiva 95/46/CE en el sentido de que existe un "recurso a medios situados en el territorio de dicho Estado miembro" cuando un buscador utilice arañas o robots para localizar e indexar la información contenida en páginas web ubicadas en servidores de ese estado miembro o cuando utilice un nombre de dominio propio de un Estado miembro y dirija las búsquedas y los resultados en función del idioma de ese Estado miembro?

1.3. ¿Puede considerarse como un recurso a medios, en los términos del art. 4.1.c de la Directiva 95/46/CE, el almacenamiento temporal de la información indexada por los buscadores en internet? Si la respuesta a esta última cuestión fuera afirmativa, ¿puede entenderse que este criterio de conexión concurre cuando la empresa se niega a revelar el lugar donde almacena estos índices alegando razones competitivas?

1.4. Con independencia de la respuesta a las preguntas anteriores y especialmente en el caso en que se considerase por el Tribunal de Justicia de la Unión que no concurren los criterios de conexión previstos en el art. 4 de la Directiva, ¿Debe aplicarse la Directiva 95/46/CE en materia de protección de datos, a la luz del art. 8 de la Carta Europea de Derechos Fundamentales, en el país miembro donde se localice el centro de gravedad del conflicto y sea posible una tutela más eficaz de los derechos de los ciudadanos de la Unión Europea?

[672] Para desarrollar este segundo tema formulan las siguientes interrogantes:

2.1. En relación con la actividad del buscador de la empresa "Google" en internet, como proveedor de contenidos, consistente en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, ¿Debe interpretarse una actividad como la descrita comprendida en el concepto de "tratamiento de datos" contenido en el art. 2.b de la Directiva 95/46/CE?.

El tercer tema consultado se cuestiona el alcance del derecho de cancelación u oposición respecto del derecho al olvido y las facultades del interesado para impedir que la información personal, aunque sea lícita, sea indexada por parte de un motor de búsqueda[673].

5.1.3. Respuesta a la consulta de prejudicialidad.

En respuesta al primer tema planteado, sobre la jurisdicción aplicable al tratamiento de datos personales en Internet, el TJUE estimó que, para efectos de determinar la competencia y la normativa aplicable, bastaba que la empresa en cuestión tuviese una oficina (la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante) en alguno de los Estados miembros. El tener la empresa Google una

---

2.2. En caso de que la respuesta anterior fuera afirmativa y siempre en relación con una actividad como la ya descrita: ¿Debe interpretarse el artículo 2.d) de la Directiva 95/46/CE, en el sentido de considerar que la empresa que gestiona el buscador "Google" es "responsable del tratamiento" de los datos personales contenidos en las páginas web que indexa?

2.3. En el caso de que la respuesta anterior fuera afirmativa: ¿Puede la autoridad nacional de control de datos (en este caso la Agencia Española de Protección de Datos), tutelando los derechos contenidos en el art. 12.b) y14.a) de la Directiva 95/46/CE, requerir directamente al buscador de la empresa "Google" para exigirle la retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información?

2.4. En el caso de que la respuesta a esta última pregunta fuera afirmativa, ¿se excluiría la obligación de los buscadores de tutelar estos derechos cuando la información que contiene los datos personales se haya publicado lícitamente por terceros y se mantenga en la página web de origen?

[673] Concretamente, la pregunta fue:

3. ¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la [Directiva 95/46] comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?.

filial en España (Google Spain) aunque no maneje directamente el Google Search, se consideraba suficiente para utilizar el derecho de la UE.

Asimismo, sobre la obligación de los motores de búsqueda para eliminar de la lista de resultados, a partir del nombre de una persona los vínculos a páginas de terceros que contienen información relativa a esta persona, aunque la publicación sea lícita, estima el TJUE que la obligaciones relativas, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento y los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias, son plenamente aplicables en razón de lo dispuesto en el artículo 25 de la Directiva 95/46/CE. Pues, agrega, estos derechos y obligaciones deben ser interpretados a la luz de los derechos fundamentales que, según reiterada jurisprudencia, forman parte de los principios generales del Derecho, cuyo respeto garantiza el Tribunal de Justicia y que están actualmente recogidos en la Carta.

En relación con el segundo tema planteado, el TJUE determinó que las autoridades de control administrativo o judiciales de los Estados podrían ordenar a los gestores de los motores de búsqueda eliminar de la lista de resultados, obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, sin que una orden en dicho sentido presuponga que ese nombre o esa información sean, con la conformidad plena del editor o por orden de una de estas autoridades, eliminados con carácter previo o simultáneamente de la página web en la que han sido publicados.

En relación con el tercer tema planteado, referido a la posibilidad del interesado de exigir al gestor de un motor de búsqueda eliminar de la lista de resultados, obtenida como consecuencia de una búsqueda efectuada a partir de su nombre, vínculos a páginas web, publicadas legalmente por terceros y que

contienen datos e información verídicos relativos a su persona, el TJUE estimó que se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados, obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que este puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general, mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si, por razones concretas, el papel desempeñado por el interesado en la vida pública, la injerencia en sus derechos fundamentales estaría justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información tratada.

5.1.4. La parte dispositiva.

De la parte dispositiva del comentado fallo del TJUE, se pueden extraer:

1. La actividad de los motores de búsqueda, la cual consiste en hallar información publicada o puesta en Internet por terceros, al indexarla de modo automático, almacenarla temporalmente y, al ponerla a disposición del público en un orden de preferencias, deber ser calificada como *tratamiento de datos personales* cuando esa información contenga datos personales, estimando al gestor de ese motor como responsable de los datos.
2. La normativa europea sobre la protección de datos personales es aplicable a las empresas que establezcan una sucursal o filial en uno de

los Estados miembros, aunque esta se dedique a otras labores como la publicidad y promoción de la empresa principal.

3. El responsable de un motor de búsqueda está obligado a eliminar de los resultados, realizados a partir del nombre de una persona, los vínculos de páginas publicados por terceros que contengan información relativa a la persona, aún en el caso en el cual la información sea lícita, pero perjudique a la persona.
4. Por último, debe examinarse en cada caso si el interesado tiene derecho a que la información en cuestión ya no está en la situación actual, lo anterior sin que esto presuponga que la inclusión en la lista de resultados, necesariamente, cause un perjuicio. Lo anterior con la salvedad de que, por razones concretas el interesado haya participado en la vida pública, caso en el cual existe un interés superior por parte del público para acceder a esa información.

En resumen, fue reconocido el derecho olvido en Internet por parte del TJUE, obligándose la empresa Google a remover las referencias del pasado del afectado, sin embargo, el medio La Vanguardia no fue obligado a remover la referencia en la cual publicó el anuncio que reclamaba el señor Costeja.

Muchos otros casos de publicaciones en Internet han generado grandes litigios en muchas partes del mundo y, ante estos, las Cortes han resuelto de formas distintas, posiblemente, como producto de los matices insertos en el concepto de privacidad.

5.2. Efectividad del derecho al olvido en Internet y el *efecto Streisand*.

El *efecto Streisand*[674] se refiere a las consecuencias de publicidad que produce la Internet cuando se ha pretendido o intentado eliminar cierto contenido o ciertos datos por diversos medios, pero no se ha logrado eliminar la información, y en su lugar se produce el efecto contrario a la censura y termina recibiendo mayor publicidad de la que habría tenido si no se hubiese tratado de ocultar o suprimir la información.

Algo similar, para que no se piense que es peor, ocurrió con la demanda de Costeja, pues si bien lo pretendido fue que se retirara de la red la información agraviante asociada con su nombre, el efecto luego de la sentencia del TJUE ha sido multiplicador, basta con escribir su nombre en Google Search y aparecen más de 21.400 resultados, siendo el primero de ellos un artículo denominado "La inolvidable historia del embargo al moroso Mario Costeja González, ocurrida en 1998"[675], que además está disponible en 17 idiomas.

Dado que en la sentencia del TJUE no se ordenó el "olvido" de la publicación original de 1998, introducida a la hemeroteca de *La Vanguardia*[676], aún es posible acudir con facilidad al artículo desde el buscador de Google, aunque no sea de

---

[674] El nombre del este concepto deriva del incidente ocurrido en el año 2003 con la actriz hollywoodense Barbra Streinsad, cuando esta demandó a un fotógrafo por haber publicado una fotografía de su casa de habitación en la costa de California. Hasta entonces la publicación de la fotografía había pasado desapercibida, pero a partir de la demanda, la fotografía se hizo viral en la red. En la actualidad la fotografía de la casa de la actriz aparece en línea.

[675] Publicado en un blog denominado *derechoaleer* del 17 de mayo de 2014, [en línea], http://derechoaleer.org/blog/2014/05/la-inolvidable-historia-del-embargo-al-moroso-mario-costeja-gonzalez-ocurrida-en-1998.html

[676] El artículo original puede ser consultado en: http://hemeroteca.lavanguardia.com/preview/1998/01/19/pagina-23/33842001/pdf.html

forma directa, la mayoría de las entradas tienen un vínculo que llevan al artículo que se pretendía fuesen borrados del resultado de las búsquedas. Es decir, si bien ya no aparece en los resultados de la búsqueda con el nombre del afectado, aparece dentro de los múltiples enlaces de los artículos que el buscador ofrece, la famosa página 23 del 19 de enero de 1998.

Pareciera que se está lejos de un derecho al olvido en Internet que sea práctico, sin embargo, se estima que los esfuerzos continuos en esta materia disminuirán el efecto Streinsad, el número de procesos administrativos y jurisdiccionales se encargarán de reducir la cantidad de noticias y comentarios, produciendo una verdadera protección de la intimidad de las personas.

Se reconoce de forma unitaria el *derecho a la protección de datos personales* como un derecho moderno, relativamente reciente, producto de las tecnologías informáticas. Este derecho deriva del derecho de intimidad y en la actualidad se vislumbra como un derecho autónomo, pero fuertemente imbricado con el derecho de intimidad.

El derecho a la protección de datos personales ha pasado por diversas etapas durante su desarrollo, si bien en un inicio estaba relacionado con el acceso a los datos personales, hoy día se proyecta como un derecho que permite el control de los datos por parte de las personas.

El contenido de protección del derecho a la protección de datos, autodeterminación informativa o libertad informática, se ha ampliado para garantizar la efectividad en un mundo cambiante, desde punto de vista tecnológico, un mundo globalizado e interconectado.

Al presentarse como un derecho que protege a las personas de los constantes ataques que sufre la *sociedad de la información,* con respecto al manejo de sus datos personales, se han ampliado los ámbitos de cobertura y tutela de este derecho, como por ejemplo, en lo que respecta al derecho de imagen, el cual se ha incluido entre los derechos a tutelar por parte del derecho a la protección de datos

personales, al considerarse que las imágenes se traducen en un conjunto de datos en las cuales una persona es identificada o identificable. También, el derecho a la privacidad de las comunicaciones se ha visto transformado puesto al pasar de comunicaciones análogas a comunicaciones electrónicas que, además no se dan en tiempo real y pueden ser almacenadas en servidores.

Las nuevas formas para procesar los datos de las personas han generado que, el derecho de protección de datos sea replanteado o reformado para dar protección ante otras circunstancias que, en principio, no podían ser consideradas. Con el advenimiento de Internet nuevos servicios se han puesto a disposición de las personas, generando así otras formas no convencionales o previstas para la recolección y procesamiento de los datos.

La velocidad del procesamiento, la capacidad informática y la interconectividad de los aparatos y servicios se han unido para crear una sociedad desde el punto de vista tecnológico muy avanzada y por ello se ha necesitado replantear algunos conceptos jurídicos para poder proteger los derechos de las personas, esencialmente su derecho a la intimidad.

Cada vez los mecanismos jurídicos de protección se tienen que hacer más fuertes desde el punto de vista legal, para poder controlar a las grandes empresas de las TIC dado que sus efectos y enlaces comerciales abarcan a una gran cantidad de países, con distintos idiomas, culturas y legislaciones. Las empresas dedicadas a los servicios relacionados con la informática y telemática han ampliado de forma ilimitada sus clientes y con ello los países en los cuales suministran sus servicios a través de Internet.

Si bien se ha iniciado con la imposición de límites a las actividades de las empresas en Internet, ello representa todo un desafío a los juristas, puesto que los problemas de jurisdicción y aplicación de los preceptos jurídicos han de ser tamizados para posibles aplicaciones, esencialmente, cuando se trata de la responsabilidad extracontractual de las empresas.

Pareciera que las personas, celosas de sus datos personales, han tomado algunas iniciativas con el propósito de proteger estos datos frente a las empresas que están deseosas de obtenerlos. Varios fueron los problemas identificados con respecto a la manipulación de los datos de las personas, problemas en el consentimiento informado, en la venta o cesión de datos, en la uniformidad de las normativas, problemas de jurisdicción, de acceso a los mecanismos jurídicos de protección, problemas con la constitución de las pruebas, en la información brindada a los usuarios, en el respeto de los derechos de la protección de los datos de las personas, se han intensificado los ataques contra los bancos de datos de las empresas y gobiernos, exponiendo a las personas que aún confían en la seguridad de los datos que ofrecen los responsables.

El costo económico de los datos y su alto valor de mercado, como se señaló, es uno de los factores que intensifica los ataques de contra las bases de datos informatizadas, a lo cual se suma la importancia en la obtención y manejo de ciertos datos para el desarrollo, principalmente, de las actividades económicas, incluidas las de los gobiernos.

En los últimos años han estado plagados de noticias sobre ataque a los datos de las personas, a través de los hackers, aplicaciones, servicios, aparatos, etc., que afectan a las personas que incluso no utilizan servicios informatizados de ninguna clase pero que utilizan los servicios necesarios estatales y comerciales, los que a su vez utilizan las facilidades que permite la informática. En este momento ni siquiera se presenta como solución que los usuarios dejen de utilizar las computadoras y aparatos celulares para no sufrir ataques, pues deberían de abandonar todos los servicios para desaparecer de todos los registros comerciales y estatales en el afán de no sufrir alguna vulneración con respecto a la manipulación de sus datos, lo cual es, en la práctica, totalmente, imposible.

Entre las posibles soluciones para aplacar la afectación de los derechos de las personas, se deben hacer reformas jurídicas, establecer controles, imponer límites y delimitar nuevas jurisdicciones, siempre en conjunto con las empresas y

gobiernos para proteger de forma efectiva los datos de las personas, incluyendo a los más despreocupados y confiados usuarios de los servicios que prestan las empresas y gobiernos en la actualidad.

Es necesario que las empresas relacionadas a los servicios de TIC colaboren con la protección de datos personales y diseñen servicios y aparatos que cuenten con mecanismos de protección a la privacidad por defecto y desde el diseño. La mayoría de los servicios y controles creados actúan cuando los derechos de las personas ya han sido vulnerados por lo cual es necesaria la integración y colaboración de las empresas. Los mecanismos jurídicos son reactivos y no preventivos lo cual representa una desventaja en la protección de los datos de las personas.

La fabricación de dispositivos que tienen sensores cuyos datos son almacenados y procesados por las empresas dejan a las personas en situaciones muy vulnerables frente a la protección de sus datos. Otros aprovechan la poca protección y desarrollo tecnológico que tienen estos dispositivos para apropiarse de datos muy valiosos de los cuales se pueden crear perfiles y patrones de las personas para luego ser vendidos en un creciente mercado.

Los corredores de datos (*data brokers*) se presentan en un mercado atractivo de la venta indiscriminada de datos de las personas a la cual se dedican más de 8000 empresas dedicadas a la elaboración de perfiles a partir de datos fragmentados pero que juntos revelan contenidos de información íntima y privada de las personas.

Como otro de los problemas que afectan a la *sociedad de la información* se presentan los programas de *Big Data,* capaces de procesar información que antes era inimaginable. La reingeniería del *software* probablemente se convierta en la cuarta revolución industrial que, sin duda catapultará a la sociedad hacia un nuevo estadio en la evolución, con ello vendrá grandes avances, pero se presenta como una gran amenaza ante la privacidad de las personas.

Las excepciones del derecho a la protección de datos personales al igual que, los derechos de privacidad e intimidad deben ser necesarias, razonables y proporcionadas, de manera que estén dispuestas por ley, sean claras y limitadas. En el momento en el cual sean aplicadas las excepciones al derecho a la protección de los datos se realice mediante una resolución debidamente fundamentada con el propósito de que existan menos arbitrariedades y la personas pueda oponerse en caso de estimar que se trata de un exceso o ilegalidad.

Aunque en la última década se han realizado esfuerzos en muchos países con el propósito de mejorar las regulaciones normativas relativas a los datos personales es necesario que se dispongan de normativas marco para la adopción de reglas comunes entre los países con el propósito de facilitar el control y la protección de los datos personales. Una de las desventajas que representa la normativa dispersa se presentan al momento en el cual se deben hacer aplicaciones de las normas por parte de los operadores del derecho se suele incurrir en errores y frente a los usuarios existe poca claridad sobre los derechos que les asisten y la forma de obtener el amparo por las violaciones de sus derechos fundamentales.

Aún nadie ha dado alguna solución de los programas que trabajan en una red paralela a Internet como la Web Profunda o Internet Profunda (*Deep Web, Dark Web, Hidden Web, Darknet*) que es imposible de rastrear por lo cual es aprovechado por los ciberdelincuentes para cometer delitos puesto que, los motores de búsqueda no pueden acceder a esta para indexar la información ahí contenida. El programa más famoso para navegar en la Internet Profunda es el creado por el proyecto Tor que facilita navegar en esta red sin ser rastreado y de forma anónima. Las autoridades, incluidas las agencias de inteligencia, aún no han encontrado alguna forma de bloquear los accesos a esta red o siquiera poder seguir los delitos que ahí se cometen.

Otros de los problemas evidenciados con la recopilación de datos y ya se ha señalado en estas conclusiones, son los problemas relacionados con el consentimiento informado que dan los usuarios para utilizar los servicios o aparatos

que tienen conexión propia o a través de los *smartphones*. Ya sea por vicios en el consentimiento o por la imposibilidad que presentan algunos artefactos en los cuales se supone que con la compra los usuarios aceptan los términos de contratos, obligándolos a políticas de privacidad que afectan sus datos personales e intimidad. La mayoría de las empresas busca obtener, con los datos de las personas, ganancias por el costo de la información ya sea vendiéndola o haciendo alianzas comerciales con otras empresas intercambiando la información que ha sido recolectada bajo contratos en los que, en apariencia, los usuarios han otorgado el consentimiento.

De otra parte, es importante que se recalque el papel de los tribunales con respecto al cumplimiento de sentencias contra grandes empresas de Internet y el efecto que esto produce en ese sito, como efecto Streisand multiplicador de la información que se pretendía borrar o suprimir, los problemas de jurisdicción y el poder económico de estas empresas frente a los usuarios de los servicios.

Por último, se quiere recordar la famosa frase Eric Schmidt, uno de los CEO de la empresa Google, que con el paso del tiempo cobra, cada vez, más relevancia al señalar que “Internet es la primera cosa que la humanidad ha construido que la humanidad no entiende, el experimento más grande de anarquía que hemos tenido”, para concluir que, el trabajo para asegurar la protección de los derechos fundamentales de las personas debe ser constante y adaptarse a las nuevas necesidades y cambios propios de un mundo globalizado e interconectado.

CUARTA PARTE. LA VIGILANCIA MASIVA Y CONCLUSIONES FINALES.

CAPÍTULO VI. VIGILANCIA MASIVA DE LOS GOBIERNOS.

"La privacidad es para los indefensos, pero la transparencia es para los poderosos".[677]

[677] Edward Snowden, ex analista de la Agencia de Seguridad Nacional de los EE.UU., frase indicada luego de las revelaciones realizadas a los medios de prensa a partir del 6 de junio de 2013.

1. CONSIDERACIONES PRELIMINARES.

El 6 de junio de 2013 el periódico, The Guardian[678] publica la primera de las denuncias acerca de la vigilancia masiva que realizaba el gobierno de los EE.UU. a través de la Agencia de Seguridad Nacional (NSA) y el gobierno del Reino Unido (RU) con su agencia homónima el Cuartel General de Comunicaciones del Reino Unido de Gran Bretaña e Irlanda del Norte (GCHQ). Un ex agente de la NSA, Edward Snowden, había dado una entrevista exclusiva en la cual revelaba información secreta de la NSA acerca de la vigilancia masiva de las comunicaciones de las personas en varios países del mundo.

Las sorprendentes noticias dieron vuelta al mundo, provocaron muchas reacciones en distintas direcciones, una sensación de desnudez y el ultraje eran los sentimientos del momento, algunos consideraban a Snowden un héroe y otros un traidor. Snowden fue perseguido por su gobierno y se giraron solicitudes de extradición en su contra. Día a día, a partir de la primera noticia, se fueron revelando más detalles de la vigilancia de las comunicaciones por parte de los gobiernos. Snowden apoyó su denuncia en documentos que pudo sustraer de la NSA, el joven analista y ex funcionario de la Agencia, se ha convertido en un fugitivo internacional.

La privacidad había sido violada en todas sus formas, era el final de la privacidad. El nombre clave del programa de vigilancia utilizado por el gobierno de los EE.UU. fue revelado, PRISM[679], siendo su nombre oficial SIGAD US-984XN. La recogida de datos sensibles más grande del mundo no necesitó una *warrant* (orden

---

[678] GREENWALD, G., "NSA collecting phone records of millions of Verizon customers daily", en *The Guardian,* 5 de junio de 2013, [diario en línea], http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[679] *Vid.* Sobre PRISM apartado *infra* Cap. VI. 2.2.

de allanamiento emitida por un Juez). La acción de vigilancia masiva pretendía justificarse en la "seguridad nacional", el programa para ese propósito fue creado en el año 2007 luego de la aprobación de la ley "Protect America Act (PAA) of 2007"[680] que reformó la ley FISA[681].

Pocos días después de la primera denuncia, el 19 de junio de 2013, el Mandatario estadounidense sale a la luz pública apoyando los programas de vigilancia por considerarlos necesarios para salvar la vida de los ciudadanos.

En este capítulo se analiza la situación legal de la vigilancia masiva y el almacenamiento de datos de las personas, se expone con detalle el marco legal en el que se sustentó el gobierno de los EE.UU. para realizar la intervención de las comunicaciones, y se reflexiona sobre las medidas y regulaciones legales necesarias para tratar de evitar la pérdida definitiva del derecho a la privacidad, ante los posibles abusos o excesos en que se ha incurrido al respecto.

La actividad e ingenio de las agencias de inteligencia para conseguir sus fines no es reciente, en el pasado, la agencia de inteligencia de RU se valió de las habilidades de Alan Turing[682] y el equipo de Bletchley Park para descifrar los códigos de los enemigos alemanes durante la Segunda Guerra Mundial. Basta una mirada al pasado para apreciar cómo las agencias de inteligencia han terminado en

---

[680] Protect America Act (PAA) of 2007, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm

[681] Foreign Surveillance Act (FISA) of 1978, 50 U.S. Code Chapter 36, [en línea], https://www.law.cornell.edu/uscode/text/50/chapter-36

[682] Como todo lo secreto por parte de las agencias de espionaje, el reconocimiento de Alan Turing como padre de las ciencias de la computación y precursor de la matemática moderna, fue realizado años luego de su muerte. Incluso fue indultado 60 años después de su muerte, recibiendo el perdón real por haber sido homosexual. Vid. OPPENHEIMER, W., Turing, condenado por gay, recibe el perdón real 60 años después de su muerte" en "*El País",* 24 de diciembre de 2013, [diario en línea], http://internacional.elpais.com/internacional/2013/12/24/actualidad/1387873660_129481.html

la vigilancia masiva, en un camino evolutivo lleno de nuevas tecnologías de espionaje y lejos de ser expuestas a la luz pública.

Se podría indicar que en términos de privacidad las revelaciones de Edward Snowden crean un antes y un después. Los expertos en derecho de la privacidad han manifestado sus primeras impresiones sobre la vigilancia masiva de Internet y las comunicaciones telefónicas. Se han iniciado casos judiciales contra estos gobiernos, las organizaciones de derechos humanos han interpuesto demandas y han realizado campañas para la protección de los derechos humanos. La cuestión principal será: si un cambio en la normativa podrá ser suficiente para proteger el derecho a la privacidad en Internet y las comunicaciones telefónicas.

En su blog el experto en seguridad Bruce Schneier[683] y crítico de los programas de vigilancia masiva del gobierno de EE.UU., señala que "*la privacidad es un derecho inherente al ser humano, y un requisito para el mantenimiento de la condición humana con dignidad y respeto*"[684], y hace una crítica al almacenamiento masivo de los datos de las personas por parte del gobierno.

[683] Chief Technology Officer of Resilient Systems, a fellow at Harvard's Berkman Center, and a board member of Electronic Frontier Foundation, (Director de Tecnología de Sistemas Resilientes, miembro de la Universidad de Harvard Berkman Center, y miembro del consejo de la EFF).

[684] "*Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect".* SCHNEIER, B., "The Value of Privacy", 19 de mayo de 2006, [en línea], https://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html

2. HISTORIA Y ORIGEN DE LA VIGILANCIA GLOBAL

2.1. Breve recuento histórico de los sistemas de inteligencia y vigilancia antes de los ataques del 9/11.

La historia de la vigilancia global se remonta al año 1940, cuando se suscribe el UKUSA Act Agreement[685] que dio origen a la red de vigilancia con el nombre codificado de ECHELON en 1971[686]. La tradición de intercambio de inteligencia entre la NSA y otras agencias de investigación tiene raíces profundas, a partir de este acuerdo y futuras enmiendas en 1946, se incorporaron a la red de vigilancia los gobiernos de Australia, Canadá y Nueva Zelanda, conformando el grupo denominado *the Five Eyes* (los Cinco Ojos), lo anterior con el propósito de compartir inteligencia.

En la actualidad este acuerdo (UKUSA) supone el inicio de una red de vigilancia que perduró por más de 70 años de forma secreta. A pesar del tiempo todavía hoy, se sabe poco acerca de la alianza y los acuerdos que unen a estos

---

[685] UKUSA Act Agreement 1940-1956 (el nombre original del acuerdo es BRUSA de las iniciales de British R.I. y U.S.A), es un acuerdo de cooperación internacional entre UK y EE.UU., firmado el 05 de maro de 1946. La historia completa del acuerdo, alcances y documentos han sido revelados por parte de la NSA luego del paso de los años que han perdido la relevancia y ahora son de acceso público. Información relacionada con este acuerdo puede ser consultable en línea en: https://www.nsa.gov/public_info/declass/ukusa.shtml

[686] ECHELON es el nombre clave utilizado por los medios de comunicación de forma global y de forma popular para referirse a los programas de inteligencia de señales (SIGINT) de recopilación y análisis de datos realizado, principalmente, por los *Five Eyes*. Un reporte completo sobre el funcionamiento de este sistema fue realizado por arte del Parlamento Europeo con el propósito de crear un Comité temporal del sistema ECHELON, [en línea], http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN

países. Pareciera que el secretismo fue uno de los principios que inspiraron estos acuerdos y ningún gobierno lo reconoció hasta después de 1999[687].

En el marco del acuerdo se establece que cada uno de los Estados parte realiza las actividades de intercepción, colección, adquisición, análisis y descifrado en cada parte del mundo y toda la información es compartida por defecto. Además, se establece en el acuerdo un centro de operaciones donde se reunirán los operativos de las múltiples agencias de inteligencia de los cinco Estados[688].

Tal y como puede desprenderse de los documentos expuestos por las agencias de seguridad e inteligencia (NSA y GCHQ)[689] la cooperación para la vigilancia es de índole militar y diplomática y, en general, están relacionadas en un inicio, con la actividad de la Unión Soviética y los bloques aliados durante la Guerra Fría. Sin embargo, pareciera necesario que se señale que los orígenes de la vigilancia masiva se remontan a los acuerdos de vigilancia militar.

Para el propósito de esta investigación se entiende por vigilancia masiva aquella actividad realizada por los estados, grandes empresas de internet y particulares, dirigida a obtener información de las personas con distintos propósitos, poniendo en riesgo en muchas ocasiones el derecho a la privacidad.

---

[687] Los acuerdos pueden ser consultados en el Archivo Nacional UK desde 2010 que fueron revelados y puestos a disposición del público por parte de la GCHQ bajo el título UKUSA Agreement, consultable en internet: http://www.nationalarchives.gov.uk/ukusa/

[688] Una guía para poder leer los documentos secretos fue puesta a disposición por parte del Archivo Nacional de UK y puede ser consultada en línea: http://www.nationalarchives.gov.uk/documents/ukusa-highlights-guide.pdf

[689] *Ibíd.*

Debe señalarse que las técnicas de vigilancia de la población han cambiado radicalmente en los últimos años, la naturaleza propia de los registros, la gran capacidad de las nuevas tecnologías y la facilidad para colectar y procesar los datos, ha permitido a los gobiernos la generación de registros automatizados sin precedentes. Uno de los peligros que representa la recolección indiscriminada de datos puede observarse en el pasado cuando los ciudadanos eran perseguidos con fines políticos, religiosos, étnicos y sociales, una historia que tiende a repetirse sobre todo en tiempos de conflictos armados o inestabilidad política[690].

En 1952 el presidente Harry Truman creó, mediante una directiva secreta, la Agencia de Seguridad Nacional NSA que permitió consolidar las actividades de vigilancia del Departamento de Defensa luego de la Segunda Guerra Mundial. Con anterioridad a la creación de la NSA existió la *Black Chamber* o Cipher Bureau MI-8 la cual operó desde 1919 hasta 1929[691].

En 1960, durante la dirección de J. Edgar Hoover, el Buró Federal de Investigación (FBI), compiló una gran cantidad de información personal de dirigentes políticos, principalmente, información de Martin Luther King, Jr., la cual era captada a través de escuchas telefónicas y micrófonos, con el objeto de

---

[690] Con base en los documentos filtrados por Snowden, se revela que la NSA ha espiado la actividad o hábitos sexuales de radicales islámicos como parte de un plan para desacreditarles. Este documento confirma la recopilación de registros de actividad sexual en línea a efectos de dañar la reputación de aquellos a los que la Agencia estima como objetivos de fuerzas radicales. En el documento se aprecian seis objetivos, todos musulmanes, con el propósito de socavar su credibilidad, reputación y autoridad. *Cfr.* USERO, A., y REILLY R.J., "Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'" en *The Huffington Post,* 26 de noviembre de 2013, [diario en línea], http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html, el documento con los nombres editados puede ser consultado en: http://i.huffpost.com/gen/1484431/original.jpg

[691] Una cronología histórica de los precedentes de la Agencia de Seguridad Nacional de los EE.UU. puede ser consultada en la página de la NSA, [en línea], https://www.nsa.gov/about/cryptologic_heritage/center_crypt_history/pre_1952_timeline/index.shtml

descubrir vulnerabilidades sexuales de estas personas y poder neutralizar a sus oponentes, como adversarios políticos, periodistas o activistas de derechos humanos.

Luego del escándalo de Watergate, el senador Frank Church condujo un comité conocido como el Comité Church (*Church Committee*) para investigar la participación de las operaciones de inteligencia federal. En ese informe se detalla el espionaje generalizado en el país y en el extranjero, y concluyó que las agencias de inteligencia han socavado los derechos constitucionales de los ciudadanos. En ese momento el Comité de inteligencia del Senado fue creado como control de las actividades de vigilancia de los EE.UU[692].

El senador Church desde 1975, había presagiado sobre los abusos de las técnicas de espionaje y los efectos que podría tener el indicar que: *"el Gobierno de los Estados Unidos ha perfeccionado una técnica que permite el monitoreo de los mensajes enviados a través del aire… esa capacidad en cualquier momento podría volverse contra el pueblo americano, y nadie volvería a tener privacidad, tal es la capacidad de monitorear todo –conversaciones telefónicas, telegramas, no importa. No existirá un lugar para ocultarse."* [693]

[692] Final report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, [en línea], https://archive.org/details/finalreportofsel01unit

[693] Senator Frank Church, Chair, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1975, en GREENWALD, G., *No place to hide,* Macmillan's, New York, 2014, [versión para lector digital Kindle].

En 1978, luego de que se revelara el informe del senador Church, se creó la Ley de Vigilancia de Inteligencia Extranjera (FISA)[694], en la cual se creó un Tribunal para estudiar las peticiones de órdenes secretas de vigilancia interna, principalmente de los extranjeros.

En el año 2001, luego de los ataques terroristas contra los EE.UU., la ley FISA toma relevancia luego de la aprobación de la Ley Patriota (USA-Patriot Act of 2001)[695], mediante la cual se ampliaron las capacidades de vigilancia de este gobiernos. La Ley Patriota modificó otras leyes principales utilizadas por parte de los organismos de inteligencia de EE.UU., relacionadas con las comunicaciones y la privacidad, incluyendo la Ley de Privacidad de las Comunicaciones Electrónicas (EPCA), que modifica el Título III de la *Omnibus Crime Control and Safe Streets Act* (the Wiretap Act), la Ley de Vigilancia de Inteligencia Extranjera de 1978 (FISA) y, la Ley de Comunicaciones de 1934.

El alcance de la vigilancia masiva de los EE.UU., incluso a lo interno de este país, aumentó luego del ataque al *Trade World Center* y el Penágono el 11 de setiembre de 2001.

Posteriormente se han realizado una serie de reformas en la legislación que han permitido a las autoridades de inteligencia acceder a los registros completos de información de llamadas telefónicas, mensajes de texto y contenidos completos de la actividad en Internet de las personas. Con base en los documentos revelados por Edward Snowden se aprecia que el contenido de los archivos al que ha podido

---

694 Foreign Surveillance Act (FISA) of 1978, 50 U.S. Code Chapter 36, [en línea], https://www.law.cornell.edu/uscode/text/50/chapter-36

695 USA-PATRIOT Act (USAPA) of 2001, Pub. L. No. 107-56, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

acceder NSA está relacionado con los correos electrónicos, chats, llamadas VOIP, archivos almacenados en la nube, entre otros[696].

En la actualidad la vigilancia masiva por parte del gobierno de los EE.UU. está justificada, legalmente, en dos de las reformas realizadas a la Ley de Vigilancia de Inteligencia Extranjera (Foreign Surveillance Act FISA) de 1978[697], en particular la realizada a la Sección 215 del Título II de la Ley Patriota (USA-PATRIOT Act USAPA) de 2001[698], y a la Sección 702 de las Enmiendas de la Ley (FISA Amendments Act FAA) de 2008[699], así como se sustenta en la Orden o Decreto Ejecutivo 12333, firmado por el ex presidente Reagan el 04 de diciembre 1981[700].

Sin embargo, luego de los documentos filtrados por Snowden ya se están gestando los cambios normativos para restringir las enormes posibilidades legales con las que cuenta la NSA para acceder de forma indiscriminada a los archivos y comunicaciones de las personas[701].

Una encuesta realizada en el mes de mayo de 2015 en los EE.UU. muestra como la mayoría de encuestados se oponen a la recopilación de datos a granel

---

[696] *Cfr.* GREENWALD, G., *No place to hide, op. cit.*, [versión para lector digital Kindle].

[697] Foreign Surveillance Act (FISA) of 1978, 50 U.S. Code Chapter 36, [en línea], https://www.law.cornell.edu/uscode/text/50/chapter-36

[698] USA-PATRIOT Act (USAPA) of 2001, Pub. L. No. 107-56, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[699] FISA Amendments Act (FAA) of 2008, 50 U.S. Code § 1881ª, [en línea], https://www.law.cornell.edu/uscode/text/50/1881a

[700] Executive Order 12333 of 1981, [en línea], http://www.archives.gov/federal-register/codification/executive-order/12333.html

[701] *Vid. Infra* Cap. VI.4.1.

realizada por parte del gobierno y dos tercios creen que no existen límites adecuados, pero al mismo tiempo apoyan el seguimiento de las comunicaciones de presuntos terroristas. En conclusión la mayoría de estadounidenses no está de acuerdo en sacrificar la libertades civiles excepto que se trate de ataques terroristas[702].

[702] *Vid.* GAO, G., "What Americans think about NSA surveillance, national security and privacy", en *Pew Research Center*, 29 de mayo de 2015, [en línea], http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/

2.2. Sistemas de vigilancia electrónica.

El secretismo de los programas de vigilancia y espionaje es, precisamente, una de las características que permite la efectividad de este tipo de actividades. Esta característica ha dificultado que se pueda obtener información completa sobre el alcance y capacidades reales de los programas de espionaje utilizados en la actualidad por parte del gobierno de los EE.UU., sin embargo a continuación se presentan algunos datos que permiten verificar los alcances de esa actividad, con cita de las las fuentes de las cuales se ha tomado la información a fin de brindar, de la forma más objetiva, la evidencia que ha sido filtrada hasta el momento.

Según los documentos filtrados por Snowden, fue la Ley denominada Protección de América (*The Protect America Act* of 2007) la que permitió, jurídicamente, a la NSA la creación de un programa secreto llamado US-984XN, también conocido como PRISM[703]. Se dice que el programa es una versión simplificada de las mismas prácticas de vigilancia que los EE.UU. estaba llevando a cabo en los años siguientes al 11 de setiembre de 2001, bajo el presidente George

[703] El programa US-984XN conocido como PRISM, es uno de los principales programas de inteligencia utilizados por la NSA, que en principio permite la recogida de datos de las empresas Microsoft, Google, Apple, Yahoo! y otros. Aún no se conocen las dimensiones y capacidades completas del programa, sin embargo, cada vez se filtran a la luz pública nuevos documentos que son analizados y han permitido determinar, al menos en parte, la capacidad operativa de este programa, que ciertamente, aún sigue siendo secreto. El gobierno de los EE.UU. insiste en que únicamente, obtienen los datos que son autorizados por parte del el Tribunal de Vigilancia de Inteligencia Extranjera. Entre los documentos revelados, hay unas diapositivas que sugieren que la NSA tiene acceso directo a la información contenida en los servidores de las empresas Google, Facebook, Apple y otros. Al efecto se puede consultar las publicaciones realizadas por The Guardian. *Cfr.* GREENWALD, G., y MACASKILL, E., "NSA Prism program taps in to user data of Apple, Google and others", en *The Guardian,* 7 de junio de 2013, [diario en línea], http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; *Cfr.* GREENWALD, G., *No place to hide, op. cit.,* [versión para lector digital Kindle].

W. Bush denominado “Programa de Vigilancia de Terroristas” (*Terrorist Surveillance Program*).

Debe advertirse que el programa PRISM es solo uno de los programas de vigilancia utilizados por parte de las agencias de inteligencia, pero según los documentos filtrados, los datos colectados por parte de este programa incluye el contenido de los correos electrónicos, chats, llamadas VOIP, archivos almacenados en la nube y más[704].

El documento principal que advierte la existencia de PRISM se basa en un grupo de 41 diapositivas, clasificadas como de alto secreto y sin distribución a los aliados extranjeros, que al parecer eran utilizadas para entrenar a agentes de inteligencia sobre las capacidades del programa. Entre las diapositivas se indica que el programa trabaja con la colaboración de las principales empresas que prestan servicios en Internet[705], sin embargo todas negaron el conocimiento del programa[706], aun así en las diapositivas se observa la fecha en la cada una de esas empresas se unió al programa.

---

[704] *Vid.* SCOTTEK, T.C. y KOPSTEIN, J., “Everything you need to know about PRISM” en *The Verge*, 17 de julio de 2013, [en línea], http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

[705] En las diapositivas se observan los logos de las empresas Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube y Apple, estas diapositivas también fueron expuestas en la publicación del abogado y periodista Glenn Greenwald “No place to hide”. *Cfr.* GREENWALD, G., *No place to hide, op. cit.,* [versión para lector digital Kindle]. Debe recordarse que Greenwald fue la primera persona contactada por Edward Snowden para iniciar sus revelaciones y quien además ha realizado varios reportajes sobre las actividades de la NSA.

[706] GREENWALD, G., y MACASKILL, E., “NSA Prism program taps in to user data of Apple, Google and others”, en *The Guardian,* 7 de junio de 2013, [diario en línea], http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Los programas utilizados por la NSA recogen dos tipos de datos: los metadatos y el contenido. Los metadatos son el subproducto de las comunicaciones, como los registros de las comunicaciones telefónicas, que revela el nombre de los participantes, la hora y el tiempo de la llamada, el número de serie del aparato telefónico, el lugar donde se encuentran y el número de teléfono de las tarjetas SIM usadas. De otra parte, los datos recogidos por PRISM incluyen el contenido de los correos electrónicos, chats, llamadas VoIP, archivos almacenados en la nube, y otros. Entre los metadatos de Internet se incluye otra información como los registros de correo electrónico, datos de geolocalización (direcciones IP) y los historiales de búsqueda web[707].

Tal y como se advirtió en el apartado anterior[708], el espionaje ha sido una actividad desplegada desde hace muchos años por parte de las agencias de inteligencia de los países. La información recabada por estas agencias ha servido de insumo para situaciones muy diversas, sustentadas la mayoría en aspectos relacionados con la seguridad, pero que también han servido para otras tareas no tan claras, tales como el control político y militar, la investigación periodística y la oposición de activistas. Ciertamente, la información colectada en épocas modernas supone una gran ventaja a quien la administre que, con las capacidades tecnológicas actuales, permiten predecir una serie de situaciones sociales que podrían transformar el mundo en aspectos políticos, sociales y económicos.

Otra de las herramientas utilizadas por parte de la NSA para la colección de datos es el programa denominado "Boundless Informant"[709] (Informante sin límites),

---

[707] *Cfr.* GREENWALD, G., *No place to hide, op. cit.,* [versión para lector digital Kindle].

[708] Vid. *Supra* Cap. VI.2.1.

[709] *Vid.* Publicación realizada por *The Guadian,* "Boundless Informant NSA data-mining tool – four key slides", del 8 de junio de 2013, en la cual se muestran las diapositivas filtradas por E. Snowden,

que proporciona la cantidad de información que ha sido colectada por parte de la agencia. En un período de 30 días se recogieron 97 billones de emails y 124 billones de registros de llamadas telefónicas alrededor del mundo[710].

Uno de los documentos filtrados muestra de forma detallada los datos recolectados por país en un período de 30 días y se muestra de la siguiente forma[711]:

Alemania (500 millones)

Brasil (2.3 billones)

India (13.5 billones)

France (70 millones)

España (60 millones)[712]

Italia (47 millones)

Holanda (1.8 millones)

Noruega (33 millones)

[en línea], http://www.theguardian.com/world/interactive/2013/jun/08/nsa-boundless-informant-data-mining-slides

[710] GREENWALD, G., *No place to hide, op. cit.,* [versión para lector digital Kindle].

[711] *Ibíd.* Dicho espionaje no registra el contenido de las llamadas, sino el número de serie de los aparatos que se comunican, el lugar donde se encuentran, el número de teléfono de las tarjetas SIM usadas y la duración de la llamada.

[712] *Vid.* GREENWALD, G. y ARANDA, G., "La NSA espió 60 millones de llamadas en España en sólo un mes" en *El Mundo*, 28 de octubre de 2013, [diario en línea], http://www.elmundo.es/espana/2013/10/28/526dcbad61fd3d07678b456b.html

Dinamarca (23 millones)

Según los datos anteriormente transcritos se estima que, la existencia de estos programas constituye una de las violaciones al derecho de intimidad más grande que haya ocurrido en la historia teniendo en consideración la cantidad de afectados, a lo que se suma el hecho de que se ha realizado en forma masiva y no individualizada.

De los documentos filtrados por Snowden, se aprecia que se utilizaron otros programas además de PRISM y *Boundless Informant*. Entre los programas que constan en estos documentos están: *PROJECT BULLRUN,* programa utilizado por la NSA en colaboración de la agencia homónima de UK GCHQ para derrotar a las formas más comunes de cifrado que se utiliza para proteger las transacciones en línea de las empresas de menor escala. EGOTISTICAL GIRAFFE, que se enfoca en el navegador de Internet Tor, que permite el anonimato en la red. MUSCULAR, un medio para invadir la privacidad de los servicios de Google y Yahoo!. X-KEYSCORE, que permite la vigilancia de las actividades en línea de una persona en tiempo real. UPSTREAM, se refiere al término utilizado por la NSA para interceptar las comunicaciones telefónicas y tráfico de datos desde la red troncal de Internet, es decir, los principales cables y conmutadores de Internet, tanto los nacionales como los extranjeros. TEMPORA, es el nombre del programa utilizado por parte de la GCHQ en cooperación con la NSA para la interceptación de las comunicaciones y contenidos de Internet. Y, finalmente, OLYMPIA, utilizado en Canadá para vigilar la actividad del Ministerio de Energía y Minas de Brasil.[713]

Según concluye Greenwald de los documentos que le facilitó Snowden, el gobierno de los EE.UU. ha construido un sistema que tiene como objetivo la eliminación total de la privacidad electrónica en todo el mundo. Lejos de ser una

[713] GREENWALD, G., *No place to hide, op. cit.,* [versión para lector digital Kindle].

exageración, el objetivo principal del gobierno ha sido constituirse en un Estado de vigilancia al colectar, almacenar, monitorear y analizar las comunicaciones electrónicas de todas las personas en todo el mundo. La NSA se dedica a una sola misión primordial: evitar que la más mínima pieza de comunicación electrónica de evada su sistémico de alcance[714].

Se estima imposible que la NSA o cualquier otra agencia de inteligencia sea capaz de leer cada correo electrónico, mensaje de texto o escuchar cada una de las conversaciones telefónicas, sin embargo, el efecto panóptico[715], creado por parte del gobierno de los EE.UU., con la vigilancia masiva se provoca que las personas se sientan vigiladas en todo momento produciendo una forma de control en la población, para asegurar el cumplimiento de las leyes o limitando conductas no deseadas. No hay duda que las personas actúan de forma distinta cuando son vigiladas o existe esta posibilidad, sin embargo, eso limita la libertad de las personas. Si bien gran parte de todo este esfuerzo de vigilancia ha sido útil para enfrentar la criminalidad, combatir el terrorismo y perseguir a los delincuentes, el uso abusivo o los excesos innecesarios hacen que se disminuyan garantías básicas de una sociedad democrática.

---

[714] *Ibíd.*

[715] Desde el siglo XVIII el filósofo y abogado inglés Jeremy Bentham introduce el concepto de la vigilancia panóptica al desarrollar una estructura modelo (panopticón) para un centro penitenciario, en el cual existe una torre central desde la cual se pueden observar todas las celdas, sin que las personas puedan saber en qué momento están siendo observadas en realidad. También, Michel Foucault estudió el modelo abstracto de una sociedad disciplinaria basada en el dispositivo panóptico en su obra *Vigilar y Castigar, Nacimiento de la prisión,* Siglo veintiuno editores Argentina, Buenos Aires, 2002.

2.3. Cooperación internacional y comercial en la vigilancia masiva.

Tal y como se ha expuesto, las actividades de espionaje y vigilancia no constituyen un fenómeno nuevo de los regímenes liberales. El escándalo suscitado por las revelaciones de Edward Snowden muestran una reconfiguración de la vigilancia que permite el acceso a los datos en gran escala, los cual supera las técnicas utilizadas en el pasado para realizar la vigilancia de las telecomunicaciones.

Pareciera que los límites y diferencias entre la vigilancia específica con fines de investigación criminal y la vigilancia a gran escala y sin objetivos claros, ahora son confusos. Estos límites entre los dos tipos de vigilancia son los que marcan la diferencia, precisamente, entre los Estados democráticos de los Estados de policía o autoritarios.

Se puede advertir que el manejo de grandes volúmenes de la información supone para los gobiernos ventajas políticas, económicas y sociales. Sin embargo, han existido alianzas entre los Estados a efectos de compartir[716] cierto tipo de información para combatir amenazas comunes como terroristas, narcotráfico y otros problemas que afectan a las sociedades modernas.

[716] Al efecto, Díaz-Caneja señala que la "voluntad de compartir es un factor clave, y que en muchas ocasiones condiciona la inteligencia disponible por los organismos de la UE, ya que actualmente se dispone de una limitada capacidad autónoma para la obtención de información, dependiendo en gran medida de la información e inteligencia que le suministran los Estados". *Cfr.* DÍAZ-CANEJA GRECIANO, J. M., "La cooperación de inteligencia en la unión europea", en *Instituto Español de Estudios Estratégicos*, No. 151/2014, p. 10.

El gobierno de los EE.UU. ha justificado la intervención de las comunicaciones en la normativa dispuesta para hacer las escuchas de los extranjeros sin necesidad de que exista una orden de juez para tales efectos[717]. Ahora bien, ¿qué sucede con los derechos de las personas extranjeras que se han visto afectadas por el empleo de técnicas de vigilancia masiva?

En las revelaciones que iniciaron en junio de 2013, se señala también la colaboración de GCHQ del Reino Unido, a través de una serie de programas y proyectos relacionados con la interceptación masiva, almacenamiento y procesamiento de datos de telecomunicaciones, dentro de los cuales resalta el programa llamado Tempora. Según los medios de prensa[718], la agencia de espionaje británica, ha interceptado los cables submarinos que transportan las llamadas telefónicas y el tráfico mundial de Internet y ha comenzado a procesar grandes cantidades de datos personales, los cuales comparte con la NSA. Además, pareciera que la intervención de las líneas submarinas fue respaldada por parte de la Agencia Nacional de Radio Defensa sueca (FRA), que ha prestado la ayuda en operaciones y programas, convirtiéndose en otro importante socio de una red de inteligencia global[719].

La evidencia que ha surgido de forma simultánea en los medio de prensa, sobre proyectos similares a los utilizados por parte de la NSA para la interceptación

---

[717] *Vid.* Foreign Surveillance Act (FISA) of 1978, 50 U.S. Code Chapter 36, [en línea], https://www.law.cornell.edu/uscode/text/50/chapter-36

[718] MACASKILL, E., *et. ál.,* "GCHQ taps fibre-optic cables for secret access to world's communications", en *The Guardian*, 21 de junio de 2013, [en línea], http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[719] NIELSEN, N., "EU asks for answers on UK snooping programme", en *EU Observer*, 26 de junio de 2013, [en línea], https://euobserver.com/justice/120656

a gran escala de datos de telecomunicaciones, involucran también a la Dirección General de Seguridad Exterior de Francia (DGSE)[720] y al Servicio Federal de Inteligencia de Alemania (BDE)[721]. Hay fuertes sugerencias para indicar que varios, si bien no todos estos, Estados miembros de la UE están participando en el intercambio de datos interceptados con servicios de inteligencia extranjeros como la NSA, lo cierto es que en algunos casos la colaboración es evidente. También Holanda, de forma reciente, ha creado una nueva Unidad de inteligencia Común Cibernética denominada "Joint Sigint Cyber Unit" (JSCU)[722].

En el estudio sobre cooperación de inteligencia que realizó Díaz-Caneja se señala como fortaleza la existencia de una estructura de inteligencia propia de la UE, pero también señala como una debilidad sus limitadas capacidades es una debilidad. Indica que, precisamente, esa limitada capacidad en inteligencia, podría ser una vulnerabilidad para los organismos europeos, ya que depende de la dependencia de la inteligencia que proporcionan los Estados[723].

Prima facie podría concluirse que algunos Estados Miembros de la UE han colaborado con los programas de vigilancia masiva utilizados por parte del gobierno de los EE.UU., sin embargo, también algunos Estados de la UE han sido objeto de la vigilancia por parte de dicho gobierno. En los primeros documentos revelados por

---

[720] FOLLOROU, J. y JOHANNES, F., "Révélations sur le Big Brother français", en *Le Monde,* 7 de julio de 2013, [en línea], http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

[721] BEUTH, V.P., "Wie der BND das Netz überwacht" en *ZEIT,* 18 de junio de 2013, [en línea], http://www.zeit.de/digital/datenschutz/2013-06/internet-ueberwachung-bnd

[722] BOON, F., *et. ál.,* "NSA infected 50,000 computer networks with malicious software" en *Nrc.nl*, de 23 de noviembre de 2013, [en línea], http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/

[723] *Cfr.* DÍAZ-CANEJA GRECIANO, J. M., *op. cit.,* p. 11.

Snowden aparece la intervención telefónica realizada a la Canciller Alemana Angela Merkel[724]. La Canciller Merkel frente esa información expresó su indignación de forma pública y solicitó a un equipo de especialistas que investigaran el caso[725].

Si bien la seguridad de las naciones debe ser un tema prioritario frente a la lucha contra la criminalidad, particularmente contra la delincuencia organizada, el narcotráfico y el terrorismo, lo cierto es que un exceso en los sistemas de vigilancia podría traer como consecuencia una debilitación en la democracia y soberanía de las naciones. Lo anterior por cuanto en los Estados miembros de la UE, la vigilancia masiva es incompatible con el régimen democrático mínimo de normas de derecho derivadas de la Carta de los Derechos Fundamentales y la Convención Europea de Derechos Humanos, que son a su vez los componentes esenciales de sus constitucionales nacionales.

El tema de la seguridad nacional tampoco es un tema aislado para las agencias de seguridad, por el contrario, dichas agencias forman parte de un sistema supranacional, democrático, que protege las libertades y los derechos fundamentales de las personas. Estas prácticas de vigilancia a gran escala y de forma indiscriminada constituyen una violación sistemática y persistente de los principios que integran la misma UE, los que se encuentran dispuestos en el artículo

---

[724] MACASKILL, E., "Germany drops inquiry into claims NSA tapped Angela Merkel's phone" en *The Guardian,* 12 de junio de 2013, [en línea], http://www.theguardian.com/world/2015/jun/12/germany-drops-inquiry-into-claims-nsa-tapped-angela-merkels-phone

[725] TRAYNOR, I., *et. ál.,* "Angela Merkel's call to Obama: are you bugging my mobile phone?", en *The Guardian,* 24 de octubre de 2013, [en línea], http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german

G del TUE[726]. Esta disposición identifica un conjunto de principios considerados como comunes a todos los Estados miembros de la UE y que incluyen, entre otros, el respeto de la democracia, el Estado de derecho y los derechos humanos.

Una alternativa propuesta por Díaz-Caneja que facilitaría la cooperación entre los Estados, es "*incorporar a todos los actores implicados al proceso de inteligencia, incluidos los solicitantes de información, los decisores, los especialistas en medios de obtención, los analistas de inteligencia, etc*"[727]. En esta alternativa, lo propuesto es centrar el objetivo común, como proceso conjunto que permita a los participantes contribuir desde sus capacidades y conocimientos.

Según el citado autor[728] esta función la podría desarrollar el Centro de Análisis de Inteligencia de la EU (INTCEN), como punto de contacto con los servicios de inteligencia de los Estado Miembros, al estar más cerca de las delegaciones del Servicio Europeo de Acción Exterior (SEAE)[729] en el extranjero y tener acceso a los informes diplomáticos de la UE.

---

[726] *Vid.* Tratado de la Unión Europea, firmado el 7 de febrero de 1992 en Maastricht, [en línea], http://europa.eu/eu-law/decision-making/treaties/pdf/treaty_on_european_union/treaty_on_european_union_es.pdf

[727] DÍAZ-CANEJA GRECIANO, J. M., *op. cit.,* p. 12.

[728] *Ibíd.*

[729] Sobre el Centro de Análisis de Inteligencia de la EU y el Servicio Europeo de Acción Exterior, se puede consultar en: http://eeas.europa.eu/archives/ashton/team/index_es.htm

2.4. Agencias de inteligencia de los EE.UU.

Con el propósito de que se tenga una idea sobre la magnitud, los alcances, el poder y los recursos destinados a la vigilancia masiva y el espionaje por parte del Gobierno de los Estados Unidos, se presenta un breve resumen de las actividades de cada una de las agencias de inteligencia que integran en su conjunto la Comunidad de Inteligencia de este Gobierno. Se trata de información oficial y además pública, que puede ser consultada en línea conforme a las fuentes que se indican en cada caso, sobre todo a través de sus respectivas páginas Web, pero que se encuentra dispersa.

Todas las agencias de inteligencia de los EE.UU., se encuentran coordinadas y son lideradas por la Oficina del Director de Inteligencia Nacional (ODNI). Mediante la Ley de Reforma de Inteligencia y Prevención del Terrorismo (Intelligence Reform and Terrorism Prevention Act of 2004, IRTPA[730]) se creó esta oficina con el propósito de mejorar, unificar y administrar los esfuerzos de la Comunidad de Inteligencia (IC). Antes de la aprobación de la IRTPA, el IC fue supervisada por el director de la CIA, quien también supervisó la Agencia Central de Inteligencia. El IRTPA fortaleció la IC definiendo aún más las metas y presupuestos, y el establecimiento de una serie de centros nacionales encargados de desarrollar métodos de colaboración para la recogida y análisis de inteligencia para un problema específico[731].

---

[730] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P. L. 108–458—dec. 17, 2004, [en línea], http://www.nctc.gov/docs/irtpa.pdf

[731] Al efecto, se puede consultar la página de los Servicio de Inteligencia del gobierno de los EE.UU. en: http://www.intelligence.gov/

Esta Comunidad de Inteligencia está estructurada para maximizar la eficacia de la recogida de datos y los esfuerzos de difusión entre todas las otras 17 agencias que dependen de esta. Cada agencia actúa bajo su propia directiva específica, todos comparten la misión de la IC para recoger y transmitir información esencial al Presidente y miembros que formulan las políticas y leyes, que requieren las fuerzas de policía y militares[732].

Le corresponde a la ODNI organizar y coordinar los esfuerzos de las otras 16 agencias que juntas integran la IC, así como gestionar la implementación del Programa Nacional de Inteligencia. El Director de esta oficina es el principal asesor del Presidente de los EE.UU. y del Consejo de Seguridad Nacional en los temas relacionados con la inteligencia de la seguridad nacional[733].

La IC se divide en tres grupos[734]:

2.4.1. *Program Managers* (Directores de Programas).

Este grupo está integrado por las agencias de más alto rango, encargadas de la gerencia de programas que asesoran y asisten a la ODNI en la identificación de necesidades, el desarrollo de los presupuestos, la gestión de las finanzas, y evaluación del desempeño de la IC.

Está compuesto por las siguientes agencias u oficinas:

---

[732] Sobre la misión y estructura de la Oficina del Director de Inteligencia Nacional (ODNI), se puede consultar en línea: http://www.intelligence.gov/mission/structure.html

[733] *Ídem.*

[734] *Ídem.*

2.4.1.1. Agencia Central de Inteligencia (CIA)[735].

La Agencia Central de Inteligencia fue creada en 1947 con la firma de la Ley de Seguridad Nacional (National Security Act of 1947[736]) en el mandato del presidente Harry S. Truman. La ley también crea un Director de Inteligencia Central (DCI) para servir como jefe de la comunidad de inteligencia de Estados Unidos, actuar como el principal asesor del presidente para asuntos de inteligencia relacionados con la seguridad nacional y servir como director de la Agencia Central de Inteligencia. La Ley de Reforma de Inteligencia y Prevención del Terrorismo de 2004 (The Intelligence Reform and Terrorism Prevention Act of 2004[737]) modificó la Ley de Seguridad Nacional para establecer un Director de Inteligencia Nacional, que asumiría algunas de las funciones anteriormente desempeñadas por el ICD, con un director independiente de la Agencia Central de Inteligencia.

2.4.1.2. Agencia de Inteligencia para la Defensa (DIA)[738].

La Agencia de Inteligencia para la Defensa, es la encargada de la inteligencia de las fuerzas armadas, diseñar la política y planificar la labor del Departamento de Defensa y la IC, apoya al gobierno en la planificación militar y operaciones de adquisición de sistemas armados. Le corresponde planificar,

---

[735] Central Intelligence Agency (CIA), www.cia.gov

[736] National Security Act of 1947, [en línea], http://www.intelligence.senate.gov/sites/default/files/laws/nsact1947.pdf

[737] Intelligence Reform and Terrorism Prevention Act of 2004, P. L. 108-458, [en línea], http://www.intelligence.senate.gov/laws/intelligence-reform-and-terrorism-prevention-act-2004

[738] Defense Intelligence Agency (DIA), www.dia.mil

gestionar y ejecutar las operaciones de inteligencia en períodos de paz, crisis y guerra.

2.4.1.3. Buró Federal de Investigación (FBI)[739].

La labor principal del Buró Federal de Investigación se centra en las amenazas a la sociedad estadounidense y en los peligros más grandes o complejos para poder ser enfrentados por las autoridades locales o estatales. Entre sus funciones principales se encuentra: la protección contra ataques terroristas, la protección contra las operaciones de inteligencia extranjeras y el espionaje, la protección contra ataques cibernéticos y delitos tecnológicos, la lucha contra la corrupción y delitos de cuello blanco, la protección de los derechos civiles y apoyo de agencias extranjeras homólogas.

2.4.1.4. Agencia de Inteligencia Geoespacial (NGA)[740].

La Agencia Nacional de Inteligencia Geoespacial, proporciona inteligencia geoespacial, referida a las características físicas y artificiales de la Tierra, interpretando la información obtenida de imágenes avanzadas. En sus inicios, en el año 1996, se conoció con el nombre de National Imagery Mapping Agency (MINA), posteriormente, en el 2003, se cambió el nombre a NGA. El avance en las tecnologías y estudio de las imágenes, han permitido la colaboración con las otras agencias de inteligencia y ha mejorado la toma de decisiones frente a cuestiones de seguridad nacional y desastres naturales. Además, la NGA gestiona un consorcio global de más de 400 relaciones comerciales y gubernamentales. El director de NGA sirve como el gerente funcional, es el jefe del Sistema Nacional de Inteligencia

---

[739] Federal Bureau of Investigation (FBI), www.fbi.gov

[740] National Geospatial-Intelligence Agency (NGA), www.nga.mil

Geoespacial (NSG) y el coordinador del Sistema Aliado mundial de Inteligencia Geoespacial (ASG).

2.4.1.5. Oficina Nacional de Reconocimiento (NRO)[741] .

La Oficina Nacional de Reconocimiento fue creada en 1961 y revelada al público en 1992. La NRO es la agencia del Gobierno de Estados Unidos a cargo del diseño, construcción, lanzamiento y mantenimiento de satélites de inteligencia de los EE.UU. Su creación en 1961 está relacionada con el lanzamiento del satélite soviético Sputnik. Junto con otros satélites del Departamento de Defensa, los sistemas NRO juegan un papel crucial en las comunicaciones del mundo, navegación de precisión, la alerta temprana de lanzamiento de misiles y el potencial de agresión militar, inteligencia de señales, y casi en tiempo real las imágenes a las fuerzas de Estados Unidos para apoyar la guerra contra el terrorismo y otras operaciones continuas.

2.4.1.6. Agencia de Seguridad Nacional (NSA)[742].

Entre las funciones principales de la NSA, se encuentran el asegurar la información de seguridad nacional sensible o clasificada frente a adversarios extranjeros y recopilar, procesar y difundir la información se “Señales de Inteligencia” con propósitos de inteligencia y contrainteligencia y apoyo a las operaciones militares.

Según se infiere de los documentos revelados por Snowden, la NSA clasifica sus programas en tres unidades, aunque estos no son necesariamente excluyentes entre sí: 1. Operaciones de Fuentes Especiales (*Special Source Operations* SSO) implican la colección abierta de acceso mediante satélites (FORNSAT), sitios de

---

[741] National Reconnaissance Office (NRO), www.nro.mil

[742] National Security Agency (NSA), www.nsa.gov

interceptación de microondas, u otras formas de colección abierta en los países de colaboradores; 2. Operaciones de Acceso Global (*Global Access Operations* GAO) requieren un acceso privilegiado a los datos que recogen, y; 3. Operaciones de Acceso Adaptado (*Tailored Access Operations* TAO) que recopilan datos con la explotación remota de ordenadores o redes. Además de estas unidades, hay una cooperación conjunta NSA-CIA llamada Servicios de Colección Especial (*Special Collection Services* SCS), que inserta el equipo en áreas que son de difícil acceso, sobre todo en las agencias diplomáticas[743].

Según las denuncias de Snowden la información colectada por parte de la NSA provine de la fuente SSO, particularmente, de la utilización del programa PRISM[744], en el cual los proveedores de servicios – incluyendo a Google, Apple, Microsoft, Facebook, YouTube, PalTalk, AOL y Yahoo – empresas que permitieron que la NSA recogiera datos de las comunicaciones o servicios para el análisis. También forman parte de SSO los programas que *pinchan* los cables de fibra óptica en todo el mundo - por lo menos parte del acceso a estos cables de fibra óptica se logra con la cooperación de la industria[745].

---

[743] Un resumen de las revelaciones realizadas por Edward Snowden aparece en la página web www.edwardsnowden.com, las referencias utilizadas en esa página refieren a las publicaciones y otros materiales que se pueden verificar siguiendo los vínculos. A efectos de hacer las referencias se utilizará el contenido del citado portal verificando la autenticidad de los contenidos y con indicación de la fuente original de publicación.

[744] BALL, J., "NSA's Prism surveillance program: how it works and what it can do", en *The Guardian*, 8 de junio de 2013, [en línea], http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google

[745] Esta información aparece mencionada en la sección titulada "Surveillance programs" del sitio web www.edwardsnowden.com, [en línea], https://edwardsnowden.com/surveillance-programs/

2.4.2. Departmental (departamentos gubernamentales).

Son componentes de IC dentro de los departamentos gubernamentales, fuera del Departamento de Defensa, los cuales se centran en atender las necesidades de inteligencia de los departamentos superiores. Está compuesto por:

2.4.2.1. Oficina de Seguridad Nacional de la Administración para el Control de Drogas (ONSI)[746].

Esta oficina fue creada en 1973 y trabaja en coordinación con otras agencias federales, estatales, locales y organizaciones de aplicación de la ley extranjera ha sido responsable de la recopilación, el análisis y la difusión de la inteligencia relacionada con las drogas. El Programa de Inteligencia de la DEA ayuda a iniciar nuevas investigaciones de las principales organizaciones de la droga, fortalece la persecución y el enjuiciamiento posterior de sus integrantes, se desarrolla la información que conduce a investigaciones y detenciones, y proporciona a los responsables políticos información de tendencias en el uso de drogas sobre las que se pueden basar las decisiones programáticas.

2.4.2.2. Oficina de Inteligencia y Contrainteligencia de Energía[747].

Esta oficina es responsable de las actividades de inteligencia y contrainteligencia del Departamento de Energía, incluyendo casi treinta oficinas de inteligencia y contrainteligencia a nivel nacional. La Oficina protege la información vital de seguridad nacional y las tecnologías, en representación de la propiedad intelectual de incalculable valor. El aporte específico a la seguridad nacional es la capacidad de aprovechar la experiencia científica y tecnológica del Departamento

---

[746] DEA's Office of National Security Intelligence (ONSI), www.dea.gov

[747] Energy Office of Intelligence & Counter-Intelligence, http://energy.gov/office-intelligence-and-counterintelligence

de Energía en apoyo de los responsables políticos, así como misiones de seguridad nacional en la defensa, la seguridad nacional, la seguridad cibernética, inteligencia y seguridad energética.

2.4.2.3. Oficina de inteligencia y análisis del Departamento de Seguridad Interna[748].

Es la oficina encargada de la inteligencia y análisis de la información que necesita el Departamento de Seguridad Interior. Promueve la identificación de amenazas a través del análisis de inteligencias, reuniendo, compartiendo y manejando la información pertinente a la seguridad nacional interior.

2.4.2.4. Oficina de inteligencia de la Guardia Costera[749].

Esta oficina ofrece apoyo a la IC, federales, estatales, locales y agencias extranjeras, proporcionando inteligencia sobre el dominio marítimo, las amenazas potenciales y las capacidades de los adversarios. Según se establece la Orden o Decreto Ejecutivo 12333, del 04 de diciembre 1981[750], corresponde a esta oficina recolectar (incluso por medios clandestinos), procesar, analizar, producir y difundir la inteligencia extranjera y contrainteligencia incluyendo la defensa e información de inteligencia para apoyar a los departamentos gubernamentales. Supervisa el desarrollo, adquisición y gestión de la inteligencia táctica, sistemas y equipos, y;

---

[748] DHS Office of Intelligence & Analysis, http://www.dhs.gov/office-intelligence-and-analysis

[749] Coast Guard Intelligence, https://www.uscg.mil/

[750] Executive Order 12333 of 1981, [en línea], http://www.archives.gov/federal-register/codification/executive-order/12333.html

lleva a cabo las relaciones de enlace de inteligencia extranjera y el intercambio de información con las agencias de inteligencia extranjeras.

2.4.2.5. Oficina de Inteligencia e Investigación del Departamento de Estado[751].

La misión principal de esta oficina es aprovechar la inteligencia para las relaciones diplomáticas de los EE.UU. Proporciona un análisis independiente de los acontecimientos. Asegura que las actividades de inteligencia apoyen fines de seguridad nacional y política exterior y realiza una labor determinante dentro del Departamento de Estado para garantizar la revisión de políticas de actividades de contrainteligencia y policiales sensibles en todo el mundo.

2.4.2.6. Oficina de Inteligencia y Análisis del Departamento del Tesoro[752].

Esta oficina se creó con el propósito de proteger mediante el análisis de la información la seguridad nacional en asunto financieros. Además analiza la información analizada es de importancia para el Departamento del Tesoro.

2.4.3. Services (servicios de inteligencia militar).

Abarcan el personal de inteligencia de las fuerzas armadas y apoyan, principalmente, sus propias necesidades de servicio. En este grupo se incluyen las

---

[751] State Bureau of Intelligence & Research, http://www.state.gov/s/inr/

[752] Treasury Office of Intelligence & Analysis, http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Intelligence-Analysis.aspx

oficinas de inteligencia de la Fuerza Aérea[753], las Fuerzas Armadas[754], Infantería de Marina[755] y la Fuerza Naval[756].

La exposición de la organización y funciones de estas agencias, revela un uso de la inteligencia y la información en diversos ámbitos extendidos, no solo a la defensa y seguridad nacional, sino hacia la política, relaciones diplomáticas y la economía.

La función y la misión de todas estas estructuras y servicios de inteligencia son vitales para la existencia y la seguridad de los Estados Unidos y en general para los países occidentales que cooperan en todo este esfuerzo. Garantizan un equilibrio frente a otras estructuras de poder dispersas en el mundo, y evitan que unas se impongan a las otras, advirtiendo de cualquier peligro que pueda surgir de los distintos movimientos sociales, políticos y militares del planeta. Asimismo, protegen las estructuras democráticas y permiten un normal funcionamiento de los estados, principalmente de aquellos que respetan el estado de derecho. Al final ello se traduce en una protección para los ciudadanos. Quizás el problema o el verdadero desafío está en reconocer cuáles deben ser los límites y cuáles deben ser los mecanismos de control necesarios para evitar los abusos y los excesos, pues son éstos los que finalmente terminan afectando los derechos de los ciudadanos, como ya ha ocurrido en el pasado, y es ahí donde surgen los verdaderos retos para los juristas.

---

[753] United States Air Force, http://www.airforce.com/

[754] United States Army, http://www.army.mil/

[755] United States Marine Corps, http://www.marines.com/home

[756] America's Navy, http://www.navy.com/

VER http://elordenmundial.com/relaciones-internacionales/los-servicios-de-inteligencia-en-el-s-xxi/

3. MARCO JURÍDICO DE LA VIGILANCIA MASIVA.

3.1. ¿Constitucionalidad y legalidad de la vigilancia masiva de los EE.UU.?

Entre los derechos contenidos en la Constitución de los EE.UU. no existe un derecho reconocido expresamente como el *right to privacy*, concepto que fue introducido por la doctrina y la jurisprudencia de la Corte Suprema, al señalar que este derecho estaba relacionado con la libertad de asociación, la integridad corporal, y las decisiones individuales acerca de la educción, la vida familiar y la sexualidad[757].

De esta manera, el desarrollo del derecho constitucional estadounidense a la privacidad se ha enfocado a entenderlo como un derecho físico, que también es oponible frente a las interferencias gubernamentales en la vida privada de las personas. La defensa de este derecho a la privacidad inició en una dimensión privativista, que refleja la forma del ordenamiento civil de ese país. La opción para quienes buscan el amparo de su derecho a la privacidad es de índole civil por lo cual el agraviante deberá responder por la responsabilidad civil extracontractual[758].

El tema de la privacidad en los EE.UU. abarca varios aspectos, los que se han regulado de forma independiente con la creación legal o estatutaria de normas relacionadas con derechos de la privacidad, entre las que destacan la privacidad en las publicaciones electrónicas, la privacidad de domicilio, la privacidad en asuntos de salud, la privacidad financiera, la privacidad de datos personales, la protección

---

[757] *Vid.* *Supra* Cap. II, apartado 3.2.

[758] *Vid.* *Supra* Cap. III, apartado 2.1.4.1.

de la privacidad de los menores en línea, la privacidad en suscripciones de video y cable, la privacidad de comunicaciones electrónicas y telefónicas, la privacidad en la educación, la privacidad en el trabajo, la privacidad en bases de datos del gobierno, etc.[759]

Tal y como se ha señalado, en los EE.UU. la ley de vigilancia electrónica está integrada por la Constitución y las leyes federales o estatales. De esta manera la Cuarta Enmienda[760], aplicable a nivel federal y a todos los estados, se debe entender como la prohibición para las agencias gubernamentales de incurrir en allanamientos y decomisos arbitrarios. Estas agencias están obligadas, en principio, a obtener con anterioridad una orden de allanamiento (*a warrant*), lo cual aplica también para los dispositivos electrónicos y otras formas de incautación de datos digitales por medio de allanamientos. La misma Constitución define "allanamiento" como el ingreso a una propiedad privada por parte de las agencias de la ley con el fin de obtener información, o bien como una intromisión del gobierno en un lugar donde una persona ha manifestado una expectativa subjetiva de intimidad que la sociedad acepta como razonable.

---

[759] Daniel Solove y Paul Schwartz realizaron un estudio actualizado sobre la normativa legal y casos jurisprudenciales relacionados con la privacidad en EE.UU. SOLOVE, D. J. y SCHWARTZ P. M., Privacy Law Fundamentals, IAPP Publications, 3era edición, New Haven, 2015.

[760] *Constitution of the United States, Amendment IV*, *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*. Constitución de los Estados Unidos, Enmienda IV. El derecho de los habitantes de que sus domicilios, documentos y efectos contra registros e incautaciones irrazonables, no sean violados, y no se podrá emitir una orden judicial de allanamiento si no existe causa probable, apoyada por juramento o protesta y particularmente describiendo el lugar para ser registrado y las personas o cosas que hay que investigar [traducción libre del autor].

De otra parte, en las leyes o estatutos federales, como la Ley de Comunicaciones Electrónicas (*Electronic Communications Privacy Act* ECPA)[761] de 1986, amplía las protecciones contenidas en la Ley federal de escuchas telefónicas de 1968, se protegen las comunicaciones de datos, video, teléfonos móviles y correo electrónico y se prohíbe la interceptación de comunicaciones transmitidas y la búsqueda de comunicaciones almacenadas.

En título I de esta normativa se refiere a la Ley de escuchas (*Wiretap Act*)[762], que regula la forma en que el gobierno puede escuchar o interceptar el contenido de comunicaciones privadas[763], incluyendo conversaciones telefónicas.

El Título II de la Ley ECPA es la Ley de Almacenamiento de las Comunicaciones (*Stored Communications Act,* SCA) [764], que regula cómo el gobierno puede acceder al contenido de las comunicaciones electrónicas (como correos electrónicos, tweets, mensajes de texto, etc.), además a otra información

---

[761] Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. § 2510-22, [en línea], https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285. Bajo este título se nombran dos leyes, he *Electronic Communications Privacy Act* y *the Stored Wire Electronic Communications Act.* De forma general protege las comunicaciones de cable, orales y las comunicaciones electrónicas, cuando se están realizando, cuando están en tránsito y cuando se almacenan en los ordenadores. La Ley se aplica a los correos electrónicos, conversaciones telefónicas, y los datos almacenados electrónicamente.

[762] Esta norma proporciona procedimientos para las autoridades de orden federal, estatal, y otros funcionarios del gobierno para obtener autorización judicial para interceptar tales comunicaciones y regula el uso y la divulgación de la información obtenida a través de escuchas telefónicas autorizadas. 18 USC § 2516-18.

[763] Un juez puede emitir una orden que autoriza la interceptación de las comunicaciones por hasta 30 días con la demostración de causa probable de que la interceptación revelará evidencia de que una persona está cometiendo, ha cometido o está a punto de cometer un "delito especial" que figuran en el § 2516. 18 USC § 2518.

[764] Stored Communications Act (SCA), [en línea], https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

no vinculada con el contenido (como por ejemplo los registros de la ubicación de la torre de celular) desde un proveedor de comunicaciones electrónicas o de almacenamiento en la nube.

Por último, en el Título III de la Ley ECPA, se incluyen las leyes de *Pen Register/Trap and Trace Device* (*Pen/Trap*)[765] regulan cómo el gobierno puede obtener información de enrutamiento y transmisión de llamadas telefónicas y otras formas de contenido electrónico, como las direcciones IP o los encabezados de los correos electrónicos.

Los Estados que conforman EE.UU., por separado tienen la facultad de regular estos temas y de ampliar la protección existente en la ley federal, sin embargo pocos Estados han incluido en forma independiente nuevas medidas para mejorar la protección a la privacidad de las personas.

Ahora bien, el problema de estas regulaciones en EE.UU. es que pareciera no existir una limitación a la cantidad de datos que se están recolectado, con el riesgo de vulnerar con ello los derechos de la Cuarta Enmienda.

En algunos precedentes jurisprudenciales, se ha interpretado la Cuarta Enmienda en el sentido de que una persona no tiene una expectativa razonable de privacidad en la información que entrega a otra persona, como un proveedor de Internet o una red social. Esto implica que la policía no tendría la obligación constitucional de obtener una orden de allanamiento para conseguir información del

---

[765] Pen Register/Trap and Trace Device (Pen/Trap), [en línea], https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206

cliente y datos de compañías como Facebook, Twitter o Google, tal y como ocurrió con los casos de Malcolm Harris[766] y Birgitta Jónsdóttir[767].

Ha de advertirse que no todas las leyes federales de los EE.UU. exigen una *causa probable* para que se permita el almacenamiento de la información, pues se aplican estándares distintos de protección a la privacidad cuando se trata de la información electrónica y digital. Pareciera que la mejor protección está contenida en la Ley de escuchas *Wiretap Act,* que requiere, además de una causa probable para la interceptación de las llamas telefónicas, la demostración por parte de las autoridades de policía que los mecanismos o procedimientos normales de investigación no han prosperado o que son peligrosos y que la comunicación (independientemente del medio) a ser interceptada tiene relación con el delito o con la persona a ser investigada.

Las otras leyes incluidas en la ECPA carecen de las protecciones de la ley de escuchas. En ese sentido la SCA permite el acceso a comunicaciones electrónicas anteriores a 180 días sin necesidad de una orden de allanamiento, el resto de comunicaciones solo puede ser intervenida con orden de allanamiento, siendo el único requisito la causa probable. De la documentación electrónica accesible a través de esta norma se encuentran las comunicaciones de más de 180 días, el contenido completo de las comunicaciones almacenadas en servidores de internet "la nube" sin necesidad de informar al afectado, y, los registros de los remitentes y destinatarios, sin incluir el contenido de la comunicación.

---

[766] *Vid.* People of the State of New York v. Malcolm Harris, Docket No. 2011NY080152 (N.Y. Crim. Ct. June 30, 2012), [en línea], https://www.aclu.org/files/assets/owsharristwitterdec63012.pdf.

[767] *Vid.* Case N° IS/01 - Birgitta Jónsdóttir, Islandia, 19 de octubre 2011, [en línea], http://www.ipu.org/hr-e/189/is01.htm

En el caso de las leyes *Pen/Trap* permiten que el gobierno obtenga información de enrutamiento (generada por las comunicaciones informáticas) si puede probar ante un juez que los datos que busca son relevantes para una investigación criminal en curso.

Entre los documentos entregados por Snowden al denunciar la vigilancia masiva se encuentra un informe de la Oficina del Inspector General de la NSA del 24 de marzo de 2009[768], en el cual se resumen las actividades de la NSA post-9/11 y, en particular, la autorización para realizar labores de vigilancia sin orden judicial emitida por el ex presidente Bush para darle facultades al Tribunal de Vigilancia de Inteligencia Extranjera.

Como se indicó antes, la vigilancia masiva por parte del gobierno de los EE.UU. se encuentra autorizada legalmente en dos de las reformas realizadas a la Ley de Vigilancia de Inteligencia Extranjera (Foreign Surveillance Act FISA) de 1978[769], en particular la realizada a la Sección 215 del Título II de la Ley Patriota (USA-PATRIOT Act USAPA) de 2001[770] y la Sección 702 de las Enmiendas de la Ley (FISA Amendments Act FAA) de 2008[771] y, adicionalmente, en la Orden o

---

[768] Informe de la Oficina del Inspector General de la NSA del 24 de marzo de 2009, documento revelado por Edward Snowden, [en línea], https://edwardsnowden.com/wp-content/uploads/2013/10/NSA-Inspector-General-Report.pdf

[769] Foreign Surveillance Act (FISA) of 1978, 50 U.S. Code Chapter 36, [en línea], https://www.law.cornell.edu/uscode/text/50/chapter-36

[770] USA-PATRIOT Act (USAPA) of 2001, Pub. L. No. 107-56, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[771] FISA Amendments Act (FAA) of 2008, 50 U.S. Code § 1881ª, [en línea], https://www.law.cornell.edu/uscode/text/50/1881a

Decreto Ejecutivo 12333, firmado por el ex presidente Reagan el 04 de diciembre 1981[772].

El problema de las leyes señaladas radica en que permitió la vigilancia de los ciudadanos estadounidenses y ciudadanos de otras partes del mundo de forma masiva, al autorizar la recolección de datos de las comunicaciones. La Corte de Vigilancia de Inteligencia Extranjera ha permitido a la NSA la intervención de telecomunicaciones, mediante la copia, escaneo y filtraciones de Internet y teléfonos a través de infraestructura física. Pese a que en la Sección 702 se prohíbe, específicamente, la intervención de comunicaciones de los ciudadanos estadounidenses, se permite la intervención sin orden judicial y de forma rutinaria de las comunicaciones.

El Tribunal de Vigilancia de Inteligencia Extranjera ha emitido ordenes muy vagas para la interceptación de comunicaciones, como la que autorizó al FBI para obtener los datos de todas las comunicaciones de la empresa Verizon en el plazo de 3 meses, incluyendo las llamadas locales[773].

La interceptación de estas comunicaciones permite la recogida de datos sin que exista una causa probable, autorizando la incautación de datos de las personas de forma indiscriminada. Las excepciones legales hasta ahora señaladas, a la protección constitucional, en especial los derechos reconocidos en la Cuarta Enmienda, parecieran excesivas y desproporcionadas, de forma tal que hacen nugatorios los derechos constitucionales de las personas, incluyendo el derecho a la privacidad, intimidad, secreto de las comunicaciones y la protección de datos

---

[772] Executive Order 12333 of 1981, [en línea], http://www.archives.gov/federal-register/codification/executive-order/12333.html

[773] Fonrein Intelligence Surveillance Court, orden de intervención de comunicaciones, documento revelado por Edward Snowden, [en línea], https://edwardsnowden.com/wp-content/uploads/2013/10/Verizon-fisa-court-order.pdf

personales. De nuevo se observa que estas medidas, si bien han sido necesarias para el mantenimiento de la democracia y la consolidación del estado de derecho, también pueden llegar a ser utilizadas con otros fines y para otros propósitos, que no se tuvieron en mente cuando fueron autorizadas, haciendo surgir un verdadero desafío para el sistema jurídico.

3.2. Reacciones y propuestas internacionales ante la vigilancia masiva.

Como se ha mencionado en diversos apartados de esta investigación, se estima que las tecnologías digitales forman una parte muy importante de la vida de las personas, han permitido mejoras considerables al acceso a la información y la comunicación en tiempo real. Adicionalmente, estas formas de comunicación han fomentado una sociedad más participativa y democrática, a través del ejercicio directo de derechos humanos y han proporcionado nuevas herramientas para documentar y denunciar amenazas y violaciones de derechos.

También, como se ha indicado, la vigilancia masiva tiene aspectos que se consideran beneficiosos, al permitir a los estados realizar verdaderas acciones de defensa del sistema político y a su vez ha permitido detectar, perseguir y combatir diversos tipos de criminalidad, en especial la delincuencia organizada, el terrorismo, el narcotráfico, la evasión fiscal, los delitos financieros y bancarios, los delitos sexuales en perjuicio de menores de edad y muchas otras formas no tradicionales de delincuencia, entre muchos otros delitos.

Sin embargo, también se ha generado una preocupación sobre la intimidad y privacidad de las personas, principalmente, con la omnipresencia de Internet y las capacidades de almacenamiento en los últimos tiempos.

La forma de operación de estas tecnologías y sus capacidades de interconexión han aumentado de forma considerable las posibilidades y capacidades para que los gobiernos, empresas y particulares puedan realizar actividades de vigilancia, interceptación y recopilación de datos. La vigilancia rutinaria, indiscriminada y, prácticamente, sin ningún tipo de controles o límites representa un grave peligro para la sociedad y, ciertamente, se traduce en una grosera violación de los derechos fundamentales de las personas.

http://www.theguardian.com/world/2013/dec/10/nsa-files-more-than-500-authors-condemn-state-surveillance

Debido a la preocupación de los líderes y representantes de los Estados Miembros de las Naciones Unidas, en el mes de diciembre de 2013 la Asamblea General aprueba la resolución 68/167[774], relacionada con el derecho a la privacidad en la era digital. Lo anterior ante la preocupación originada por las revelaciones publicadas en 2013 sobre las tecnologías que permiten acceder a gran parte del tráfico mundial en Internet, a los registros de llamadas en los Estados Unidos y otros países, las libretas de contactos electrónicos de los particulares y enormes volúmenes de otros contenidos digitales de comunicación, realizadas a través de la NSA y el GCHQ.

También en esta resolución (68/167) la Asamblea General solicitó a la Alta Comisionada de las Naciones Unidas para los Derechos Humanos que presentase, al Consejo de Derechos Humanos y a la Asamblea General, un informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales y la recopilación de datos personales en los planos nacional y extraterritorial, incluso a gran escala, que incluyera opiniones y recomendaciones para que lo examinaran todos los Estados Miembros.

De esta forma, la Oficina del Alto Comisionado (ACNUDH) elaboró el informe solicitado en conjunto con la Universidad de las Naciones Unidas, investigando la aplicación del derecho internacional de los derechos humanos a los regímenes nacionales de control de la vigilancia digital por parte de los gobiernos. Para la

[774] Asamblea General, Naciones Unidas, Resolución 68/167, 18 de diciembre de 2013, [en línea], http://www.un.org/es/comun/docs/?symbol=A/RES/68/167

elaboración de ese informe, la ACNUDH realizó un cuestionario para los Estado Miembros, a través de sus Misiones Permanentes en Ginebra y Nueva York, las organizaciones internacional y regionales, las instituciones nacionales de derechos humanos, las organizaciones no gubernamentales y entidades empresariales[775].

En el informe de la ACNUDH[776] se expresa la preocupación por la proliferación de la vigilancia digital abierta y encubierta en jurisdicciones de todo el mundo, y se evidencia como se ha convertido esta vigilancia masiva en un hábito en lugar de mantenerse como una medida de tipo excepcional.

De forma general se destacan en el informe los ejemplos de la vigilancia digital y se incluyen los casos en los cuales los gobiernos han amenazado con prohibir los servicios de empresas de telecomunicaciones, a menos que cooperen con el acceso a la información del tráfico de datos, los casos que han utilizado la información para atacar a los opositores políticos o disidentes y los casos en los cuales se ha solicitado a las empresas que revelen la información de los clientes y

---

[775] El cuestionario y las contribuciones aportadas, pueden consultarse en: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx. Conviene que se mencione que en muchas de estas contribuciones se expusieron en detalle los marcos legislativos nacionales existentes y otras medidas adoptadas para asegurar el respeto y la protección del derecho a la privacidad en la era digital, así como las iniciativas emprendidas para establecer y poner en práctica garantías procesales y una supervisión efectiva. En algunas de las contribuciones se expusieron los obstáculos encontrados al tratar de hacer efectivo el derecho a la privacidad en la era digital y se sugirieron, entre otras, las siguientes iniciativas a nivel internacional: alentar al Comité de Derechos Humanos a actualizar sus observaciones generales pertinentes, en particular sobre el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos; y la creación por el Consejo de Derechos Humanos de un mandato de los procedimientos especiales sobre el derecho a la privacidad y la participación de los titulares de los procedimientos especiales pertinentes en iniciativas conjuntas o individuales para abordar las cuestiones relacionadas con el derecho a la privacidad en el contexto de la vigilancia digital y para proporcionar orientación sobre las buenas prácticas.

[776] *Vid.* Informe de la Oficina del Alto Comisionado de Naciones Unidas de Derechos Humanos, del 30 de junio de 2014, sobre el derecho a la privacidad en la era digital, [en línea], http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

empleados. Sin embargo, también se destaca la necesidad de la vigilancia electrónica en casos necesarios para hacer cumplir la ley o por razones de inteligencia y se plantea la necesidad de implementar medidas internacionales más fuertes para garantizar la privacidad de las personas.

De otra parte, la Vicepresidenta de la Comisión Europea y Comisaria de Justicia, Viviane Reding, durante una entrevista concedida al diario griego Naftemporikien, declaró que "*la UE necesita crear una Agencia Europea de Inteligencia para el 2020, la cual reforzaría las relaciones entre los servicios de inteligencia de los estados miembros*"[777], lo anterior fue manifestado como reacción ante las noticias de la vigilancia masiva realizadas por parte de la NSA y GCHQ.

En ese mismo sentido se pronunció el profesor de Ideas Políticas y Teoría de la Guerra de la Universidad Humboldt de Berlín, Herfried Münkler, al manifestar que "*nuestros servicios de espionaje están en una situación de dependencia respecto a los estadounidenses y que la condición de países amigos no garantiza que nuestros intereses ni los derechos de nuestros ciudadanos sean respetados*", continuó señalando que "*El Gobierno alemán ha descubierto un nuevo concepto a defender, la soberanía digital, pero no sabe muy bien cómo hacerlo. Yo digo que Alemania no lo puede hacer en solitario y que necesitamos una NSA europea*"[778], lo anterior también fue manifestado a propósito de las noticias divulgadas sobre el espionaje y la vigilancia masiva realizados por parte del gobierno de los EE.UU.

---

[777] GIANNOULIS, K., "Europe needs to strengthen cross-national intelligence cooperation", en *Neweurope,* 4 de noviembre de 2013, [en línea], http://www.neurope.eu/article/reding-eu-needs-european-intelligence-agency/

[778] SANCHEZ, R., "Necesitamos un servicio de inteligencia europeo", en *El mundo,* 15 de agosto de 2014, [en línea], http://www.elmundo.es/internacional/2014/08/15/53edf27eca47418a468b457e.html

En noviembre de 2013 el Consejo de la Unión Europea emitió un comunicado relacionado con las políticas de defensa y seguridad común, en el cual se expuso que, con el fin de hacer frente a las amenazas a la seguridad, tanto a las tradicionales como a las nuevas, la UE tiene que aplicar y desarrollar aún más su enfoque integral para todas las fases de un conflicto, desde la alerta temprana y la prevención, hasta la estabilización y consolidación de la paz[779].

Debe recordarse que, en el mes de febrero de 2004, ya se había planteado la idea de la creación de una Agencia de Inteligencia Europea, los Estados de Austria y Bélgica propusieron la creación de una Agencia Central de Inteligencia Europea a efectos de coordinar los diferentes servicios de inteligencia de los Estados miembros. Según la propuesta, esta agencia debería convertirse en un centro de análisis y evaluación a nivel europeo y mundial, en especial en las áreas de terrorismo y armas de destrucción masiva. CITA

[779] Conclusiones del Consejo de la Unión Europea relativas a la Política Común de Seguridad y Defensa, 25 de noviembre de 2013, [en línea], http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/139719.pdf

3.3. Normativa internacional de Derechos Humanos y la vigilancia masiva.

La normativa internacional de los derechos humanos proporciona un marco jurídico universal para evaluar toda injerencia en los derechos individuales, entre los que desataca el derecho a la privacidad. Debe advertirse la existencia de fuertes tensiones entre los programas de vigilancia masiva, llevados a cabo por algunos Estados, con la existencia de compromisos internacionales y, en algunos casos, hasta fundacionales, de todas maneras, compromisos adquiridos de forma previa entre los Estados, en los cuales, de forma previa se reconocen derechos individuales como la protección a la privacidad de las personas.

Si bien la vigilancia electrónica es necesaria y justificada en algunas ocasiones se aplica dentro de la legalidad del derecho internacional de los derechos humanos, como una medida indispensable y eficaz, cuando persiguen fines legítimos de las fuerzas de policía o inteligencia, existe un gran margen de duda para establecer si la vigilancia electrónica a granel es compatible con esas normas jurídicas internacionales, es decir en qué momento esta vigilancia podría ser arbitraria o ilegal, de forma que vulnere el derecho de intimidad personal, invadiendo la vida privada de los ciudadanos, la familia, el domicilio o las comunicaciones, definición difícil de establecer, al menos a priori, lo que dificulta aún más que los gobiernos se planteen la posibilidad de tomar medidas concretas para proteger a sus habitantes contra tales injerencias en los derechos fundamentales de las personas.

Como O´Donnell ha argumentado, el Estado de Derecho no sólo debe entenderse como una característica genérica de los sistemas legales y del desempeño de los tribunales de justicia, sino también como uno de los pilares

básicos de un Estado democrático, que protege derechos fundamentales limitando con ello la actividad discrecional o "excepcional" de las autoridades estatales[780].

De acuerdo al concepto del "estado de derecho democrático", un sistema legal tiene que ser en sí mismo democrático, para ello deben crearse mecanismos de rendición de cuentas y supervisión, en el seno del sistema de un poder judicial independiente, un sistema que sea capaz de mantener la actividad de las instituciones internas no solo dentro del marco legal sino también dentro de los principios propios de la democracia, principalmente, en lo que respecta al principio de proporcionalidad.

En este sentido pareciera que la noción de "seguridad nacional" que han utilizado algunas comunidades de inteligencia y algunos gobiernos no corresponde a la comprensión democrática de la seguridad nacional según lo previsto en los sistemas constitucionales democráticos, donde un elemento clave de la constitucionalidad permanece en el control judicial efectivo y supervisión de las acciones del Poder Ejecutivo, entre las que se incluyen los límites de la seguridad nacional del Estado.

En el marco jurídico internacional existen varias disposiciones normativas que regulan el derecho de intimidad de las personas, como el artículo 12 de la Declaración Universal de Derechos Humanos que establece que *"nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su*

---

[780] O'DONNELL, G., "La irrenunciabilidad del Estado de Derecho", en *Revista Instituciones y Desarrollo*, No. 8 y 9, Institut Internacional de Governabilitat de Catalunya, Còrsega, Barcelona, 2001, pp. 1-24.

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"[781].

De igual forma, el Pacto Internacional de Derechos Civiles y Políticos, establece en su artículo 17 que *"nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación"*. Afirma además que *"toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"*[782].

En este mismo sentido, el artículo 8.1 de la Convención Europea para la protección de los Derechos Humanos y de las Libertades fundamentales de 1950, señala que "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*" [783].

Sobre el derecho de intimidad varios organismos internacionales y regionales de derechos humanos se han pronunciado, brindando lineamientos relacionados con este derecho. En ese sentido el Comité de Derechos Humanos ha indicado que el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos exige la protección respecto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, así como de ataques ilegales a su honra y reputación. Por lo cual, este derecho debe estar garantizado respecto de todas

---

[781] *Vid.* Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948, [en línea], http://www.un.org/es/documents/udhr/

[782] *Vid.* Pacto Internacional de Derechos Civiles y Políticos de 1966, [en línea], http://www.unhchr.ch/spanish/html/menu3/b/a_ccpr_sp.htm; Este Pacto fue firmado por los EE.UU. el 5 de octubre de 1997, pero no ha sido ratificado.

[783] Convención Europea para la protección de los Derechos Humanos y de las libertades fundamentales, [en línea], http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/SpanishEspagnol.pdf

esas injerencias y ataques, provengan de las autoridades estatales o de personas físicas o jurídicas. Las obligaciones impuestas por este artículo exigen que el Estado adopte medidas legislativas y de otra índole para hacer efectivas la prohibición de esas injerencias y ataques y la protección de este derecho[784].

Así mismo, de forma expresa indicó el citado Comité que *"como todas las personas viven en sociedad, la protección de la vida privada es por necesidad relativa. Sin embargo, las autoridades públicas competentes sólo deben pedir aquella información relativa a la vida privada de las personas cuyo conocimiento resulte indispensable para los intereses de la sociedad en el sentido que tienen con arreglo al Pacto. En consecuencia, el Comité recomienda que los Estados señalen en sus informes las leyes y reglamentos que regulan las injerencias autorizadas en la vida privada"*[785].

Tal y como se ha señalado en varios de los apartados de esta investigación, las técnicas de vigilancia masiva empleadas por algunos gobiernos también pueden afectar otros derechos fundamentales, tales como el secreto a las comunicaciones, la protección de la persona frente al tratamiento de sus datos personales, la libertad de expresión, la libertad de asociación y el derecho a la vida familiar.

---

[784] Observación General No. 16, Comentarios generales adoptados por el Comité de los Derechos Humanos, Artículo 17 - Derecho a la intimidad, 32º período de sesiones, U.N. Doc. HRI/GEN/1/Rev.7 at 162 (1988), [en línea], http://www1.umn.edu/humanrts/hrcommittee/Sgencom16.html

[785] *Ibíd*. De igual forma, recomienda el Comité que *"la recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley. Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y por que nunca se la utilice para fines incompatibles con el Pacto"*.

Conviene advertir que los datos capturados por parte de las agencias de inteligencia, si bien podrían no utilizarse, la mera posibilidad de que puedan captarse crea una injerencia en la vida privada y puede tener un efecto negativo en los derechos de las personas[786].

En ciertos supuestos las injerencias o las limitaciones del derecho a la intimidad podrían justificarse en el tanto estas sean excepcionales, necesarias, legales y proporcionales, pues de lo contrario se afectarían los derechos fundamentales de las personas. Como todo derecho la intimidad posee restricciones y, pero estas no podrían ser arbitrarias o ilegítimas[787].

En la normativa Internacional de Derechos Humanos no se indican de forma expresa limitaciones o excepciones al derecho de intimidad. Sin embargo, la Comisión de Derechos Humanos de la ONU también ha señalado algunas reglas generales para la limitación y desaplicación del Pacto Internacional de Derecho Civiles y Políticos en los Principios de Siracusa[788]. En esa oportunidad, los representantes de los Estados participantes estuvieron de acuerdo en la necesidad de proceder a un examen minucioso de las condiciones y los motivos para las limitaciones y derogaciones permisibles enunciadas en el Pacto a fin de lograr una

---

[786] *Vid.* *Infra* Cap. VI.2.2., sobre el efecto panóptico de la vigilancia; *v. et.*, Tribunal Europeo de Derechos Humanos, *Weber and Saravia v. Germany* de 2006, párr. 78 y *Malone v. UK* de 1984, párr. 64.

[787] *Vid.* Observación General No. 16, Comentarios generales adoptados por el Comité de los Derechos Humanos, Artículo 17 - Derecho a la intimidad, 32º período de sesiones, U.N. Doc. HRI/GEN/1/Rev.7 at 162 (1988), [en línea], http://www1.umn.edu/humanrts/hrcommittee/Sgencom16.html

[788] Principios de Siracusa sobre las Disposiciones de Limitación y Derogación del Pacto Internacional de Derechos Civiles y Políticos, Comisión de Derechos Humanos 41º Período de sesiones, temas 18 del programa provisional, 24 de agosto de 1984, [en línea], http://www.derechos.org/nizkor/excep/siracusa84.html

aplicación efectiva del régimen de derecho. De forma general, los participantes estuvieron de acuerdo en que existe una estrecha relación entre el respeto de los derechos humanos, el mantenimiento de la paz y la seguridad internacional. Además, estimaron que la violación sistemática de los derechos humanos socava la seguridad nacional y el orden público y puede constituir una amenaza a la paz internacional[789].

Entre las cláusulas de limitación del Pacto Internacional de Derecho Civiles y Políticos acordados en Siracusa, se incluyeron algunas relacionadas con la seguridad nacional, por lo que conviene se mencionen de forma expresa para ilustrar en cuáles casos podrían limitarse o derogarse los derechos reconocidos en ese Pacto, para tener un parámetro sobre los límites y excepciones de los derechos fundamentales.

La cláusula 5 del citado Pacto Siracusa señala que únicamente se puede limitar el ejercicio de los derechos humanos si lo permite una ley nacional. De esta manera la cláusula 6 indica que la limitación no puede ser arbitraria o irrazonable y se tienen que ofrecer mediante ley recursos adecuados y eficaces contra la imposición ilegal o abusiva de limitaciones de derechos humanos, lo que se dispone en la cláusula 7.

Concretamente y bajo el título de seguridad nacional se exponen en el Pacto de Siracusa cuatro cláusulas sobre los límites y excepciones de los derechos fundamentales en los casos en los cuales se invoque la seguridad nacional. De esta forma se señala:

"19. Solamente se puede invocar la seguridad nacional para justificar las medidas que limiten ciertos derechos cuando estas medidas se adopten para

---

[789] *Ibíd.*

proteger la existencia de la nación, su integridad territorial o su independencia política contra la fuerza o la amenaza de la fuerza.

20. No se podrá invocar la seguridad nacional como motivo para imponer limitaciones o impedir amenazas puramente locales o relativamente aisladas contra el orden público.

21. No se podrá utilizar la seguridad nacional como pretexto para imponer limitaciones vagas o arbitrarias y solamente se podrá invocar cuando existan garantías adecuadas y recursos eficaces contra los abusos.

22. La violación sistemática de los derechos humanos socava la seguridad nacional y puede poner en peligro la paz y la seguridad internacionales. Un Estado que sea responsable de una violación de este tipo no podrá invocar la seguridad nacional para justificar las medidas encaminadas a suprimir la oposición a dicha violación o a imponer prácticas represivas contra su población."[790]

Entonces, según lo expuesto, se puede invocar la seguridad nacional como una forma válida para reducir o suspender los derechos protegidos en el Pacto Internacional de Derecho Civiles y Políticos, siempre y cuando esté reconocido por una ley nacional (cláusula 5), se justifique en la seguridad nacional para proteger la existencia de la nación, su integridad territorial o su independencia política contra la fuerza o la amenaza de la fuerza (cláusula 19). Ahora bien, no podrían justificarse las limitaciones en la seguridad nacional cuando se trate de amenazas locales (cláusula 20) o cuando esas limitaciones sean arbitrarias y no se cuente con garantías adecuadas y recursos eficaces contra los abusos (cláusula 21).

En la Parte II del Pacto de Siracusa se exponen, bajo el título de "derogaciones en situaciones excepcionales", algunas circunstancias que justifican las limitaciones a los derechos fundamentales cuando se pongan en peligro la vida de la nación". Conforme a esta tesis se entiende que:

---

[790] Principios de Siracusa sobre las Disposiciones de Limitación y Derogación del Pacto Internacional de Derechos Civiles y Políticos, *op. cit.*, cláusulas 19-22 bajo el título de "seguridad nacional".

Un Estado parte se enfrenta con una situación excepcional y un peligro real o inminente que amenace la vida de la nación en dos situaciones:

a. Cuando afecte a toda la población y a todo el territorio del Estado o parte de él, y

b. Cuando amenace la integridad física de la población, independencia política o la integridad territorial del Estado o la existencia o el funcionamiento básico de instituciones indispensables para asegurar y proteger los derechos reconocidos en el Pacto.

De esta manera, señala el citado Pacto, el conflicto interno y la agitación que no representen una amenaza grave e inminente a la vida de la nación no pueden justificar las derogaciones en virtud del artículo 4, así como las dificultades económicas por sí solas no pueden justificar las medidas de derogación.

Este Pacto señala también las condiciones que debe cumplir un Estado que suspenda los derechos, según se indica en los siguientes requisitos[791]:

"1. Un Estado parte que suspenda sus obligaciones en virtud del Pacto hará una proclamación oficial de la existencia de una situación de excepción que amenaza la vida de la nación.

2. Los procedimientos para proclamar un estado de excepción en virtud del derecho nacional se establecerán antes de que se produzca el estado de excepción.

3. Un Estado parte que suspenda sus obligaciones en virtud del Pacto comunicará inmediatamente a los demás Estados partes en él, por conducto del Secretario General de las Naciones Unidas, las disposiciones que ha derogado y los motivos por los que lo ha hecho.

---

[791] Principios de Siracusa sobre las Disposiciones de Limitación y Derogación del Pacto Internacional de Derechos Civiles y Políticos.

4. La notificación contendrá suficiente información para que los Estados partes puedan ejercer sus derechos y cumplir sus obligaciones en virtud del Pacto. En particular incluirá:

a. las disposiciones del Pacto que han sido derogadas;

b. un ejemplar de la proclamación del estado de excepción junto con las disposiciones constitucionales, la legislación o los decretos que rijas el estado de excepción para ayudar a los Estados partes a comprender el alcance de la derogación;

c. la fecha efectiva de la imposición del estado de excepción y el período para el que ha sido proclamado.

d. Una explicación de los motivos que indujeron al gobierno a adoptar la decisión de derogar las disposiciones con una breve descripción de las circunstancias que llevaron a la proclamación de estado de excepción

e. Una breve descripción del efecto previsto de las medidas de derogación sobre los derechos reconocidos por el Pacto, con copias de los decretos proclamados antes de la notificación por lo que se suspenden esos derechos.

5. Es posible que los Estados partes pidan que se les facilite más información por medio del Secretario General para poder cumplir con sus obligaciones en virtud del Pacto

6. Un Estado parte que no notifique inmediata y debidamente su derogación incumple sus obligaciones para con los demás Estados partes y puede ser privado de las defensas que de otra forma dispondría en virtud de los procedimientos previstos el Pacto.

7. Un Estado parte que haga uso del derecho de derogación según lo dispuesto en el artículo 4 pondrá fin a la misma en el plazo más breve que sea necesario para acabar con el estado de excepción que amenaza la vida de la nación.

8. En la fecha en que ponga fin a dicha derogación, el Estado parte la notificará a los demás Estados partes por conducto del Secretario General de las Naciones Unidas.

9. Una vez que se ha puesto fin a la derogación impuesta de conformidad con el artículo 4 deberán restablecerse plenamente todos los derechos y libertades

protegidos por el Pacto. Tan pronto como sea posible, deberán examinarse las secuelas de las medidas de derogación. Deberán adoptarse medidas para remediar las injusticias y compensar a las víctimas de esta injusticia mientras duraron las medidas de derogación o a consecuencia de ellas."

De otra parte, el Comité de Derechos Humanos de Naciones Unidas ha señalado que los Estados parte deben abstenerse de violar los derechos reconocidos por el Pacto y que "*cualesquiera restricciones a cualquiera de esos derechos debe ser permisible de conformidad con las disposiciones pertinentes del Pacto. Cuando se introducen restricciones, los Estados deben demostrar su necesidad y adoptar únicamente las medidas que resulten proporcionales a la consecución de los legítimos objetivos para lograr una protección constante y eficaz de los derechos del Pacto*"[792]

A partir de las indicaciones señaladas por dicho Comité de Derechos Humanos y las cláusulas de Siracusa, podría señalarse que en esencia las limitaciones de los derechos fundamentales requieren que se autoricen en forma expresa mediante una ley, la cual debe ser clara, accesible y precisa. La limitación debe ser necesaria en el sentido de lo que se pretende alcanzar como objetivo legítimo y debe ser proporcional al objetivo, eligiendo la opción menos lesiva a los derechos de las personas. También es necesario que los Estados que adopten estas medidas demuestren que la limitación está relacionada con un objetivo legítimo. En todo caso las limitaciones no podrían vaciar de contenido los derechos humanos protegidos. Ahora bien, ¿qué pasaría si las limitaciones no cumplen con esos enunciados? En principio se estaría en presencia de limitaciones arbitrarias e ilegítimas.

---

[792] *Vid.* Observación General No. 31, Comentarios generales adoptados por el Comité de los Derechos Humanos de Naciones Unidas, La índole de la obligación jurídica general impuesta, 80º período de sesiones, U.N. Doc. HRI/GEN/1/Rev.7 at 225 (2004), [en línea], http://www1.umn.edu/humanrts/hrcommittee/Sgencom31.html

En el caso concreto de la vigilancia electrónica de forma masiva, pareciera que no se ajusta a los principios o reglas generales para la limitación de los derechos humanos, en particular el derecho a la privacidad. Debe advertirse que, si bien este caso pareciera no cumplir con los enunciados para la limitación legítima de derecho fundamentales, talvez la objeción principal radica en la proporcionalidad de la medida. En ese sentido todos los datos recogidos por parte de las agencias de inteligencia, autoridades del gobierno y empresas privadas, en principio podrían llegar a constituir una violación directa del derecho a la intimidad, el secreto de las comunicaciones y la protección de los datos personales, excediendo con ello el objetivo o fin para el cual han sido colectados, porque aún no se sabe quién tiene acceso a esos datos, cómo podrían llegar a ser foltrados y qué usos posteriores se dará a toda esa información.

De esta manera, cualquier programa de vigilancia debe realizarse con base en la ley, la que debe dictarse de conformidad con los requerimientos constitucionales nacionales y el derecho internacional de los derechos humanos. Según se señala en el Informe de la Oficina del Alto Comisionado de Naciones Unidas de Derechos Humanos, sobre el derecho a la privacidad en la era digital, *"el Estado debe asegurar que toda injerencia a la intimidad y privacidad de las personas esté autorizada mediante leyes que: a) sean de acceso público; b) contengan disposiciones que garanticen que la obtención, el acceso y la utilización de los datos de las comunicaciones obedezcan a objetivos específicos legítimos; c) sean suficientemente precisas y especifiquen en detalle las circunstancias concretas en que dichas injerencias pueden ser autorizadas, los procedimientos de autorización, las categorías de personas que pueden ser sometidas a vigilancia, el límite de la duración de la vigilancia y los procedimientos para el uso y el almacenamiento de*

los datos recopilados; y d) proporcionen salvaguardias efectivas contra el uso indebido"[793].

Asimismo, parece necesario que se advierta que algunos Estados tampoco han adoptado medidas efectivas para proteger a las personas sujetas a su jurisdicción, contra las prácticas de vigilancia ilegales de otros Estados o entidades comerciales, en contravención de sus propias obligaciones en materia de derechos humanos. Lo anterior pese a que el Pacto Internacional de Derechos Civiles y Políticos[794] establece que cada uno de los Estados partes se compromete a respetar y a garantizar, a todos los individuos que se encuentren en su territorio y estén sujetos a su jurisdicción, los derechos reconocidos en el Pacto, sin distinción alguna de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social.

Esto quiere decir que un Estado está obligado a respetar y garantizar los derechos establecidos en el Pacto a todas las personas sometidas a su poder o a su control efectivo, incluso si estas personas no se encuentran en su territorio. Esa obligación también se debe entender como extensiva a todas las personas que de alguna manera se encuentran sometidas a la autoridad de ese Estado. De lo contrario, podría entenderse que se permite a los Estados eludir las obligaciones internacionales, en materia de derechos humanos, mediante la adopción de medidas fuera de su territorio que tendría prohibido tomar en su propia jurisdicción.

En ese sentido apunta Wong que *"Los derechos fundamentales a la privacidad y la libertad de expresión que son tan sagrados para los estadounidenses*

---

[793] *Vid.* Informe de la Oficina del Alto Comisionado de Naciones Unidas de Derechos Humanos, *op. cit.,* pár. 28.

[794] *Vid.* Art. 2 del Pacto Internacional de Derechos Civiles y Políticos.

no son menos valiosos para los ciudadanos de otros países, por lo que tampoco ellos deberían ser objeto de la vigilancia masiva. Es urgente que se aprueben reformas integrales a la vigilancia para ir más allá de los arreglos parciales"[795]

Expuesto de otra forma, los Estados no pueden eludir sus responsabilidades en materia de derechos humanos, limitándose a mantener esas potestades fuera del alcance de sus propias leyes. No parecieran aceptables las justificaciones dadas por las agencias de inteligencia al señalar que la vigilancia masiva no se realizó a ciudadanos estadounidenses, limitándose a la interceptación y vigilancia de extranjeros de conformidad con la Ley FISA, pues el derecho internacional de los derechos humanos de forma explícita, en relación con el principio de no discriminación[796], indica que todas las personas son iguales ante la ley.

Esto ha sido reforzado por el Comité de Derechos Humanos de Naciones Unidas ha señalado la importancia de adoptar medidas para que toda interferencia en el derecho a la intimidad se ajuste a los principios de legalidad, proporcionalidad y necesidad, con independencia de la nacionalidad o el emplazamiento de las personas cuyas comunicaciones estén bajo vigilancia directa.

---

[795] WONG, C., "EE.UU.: Un paso modesto para frenar los excesos del espionaje" *en Human Rights Watch,* 3 de junio de 2015, [en línea], https://www.hrw.org/es/news/2015/06/03/eeuu-un-paso-modesto-para-frenar-los-excesos-del-espionaje

[796] El artículo 26 del Pacto Internacional de Derechos Civiles y Políticos dispone que *"todas las personas son iguales ante la ley y tienen derecho sin discriminación a igual protección de la ley"* y añade que, *"a este respecto, la ley prohibirá toda discriminación y garantizará a todas las personas protección igual y efectiva contra cualquier discriminación por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social"*. De igual forma, el artículo 17, que establece que *"nadie será objeto de injerencias arbitrarias o ilegales en su vida privada"* y que "*toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"*.

Asimismo, señala este Comité, debe asegurarse de que cualquier interferencia en el derecho a la intimidad, la familia, el hogar o la correspondencia esté autorizada por leyes, y que estas: i) sean de acceso público; ii) contengan disposiciones que garanticen que la obtención, el acceso y la utilización de los datos de las comunicaciones obedezcan a objetivos específicos legítimos; iii) sean suficientemente precisas y especifiquen con detalle las circunstancias concretas en que estas interferencias pueden ser autorizadas, los procedimientos de autorización, las categorías de personas que pueden ser sometidas a vigilancia, el límite de la duración de la vigilancia y los procedimientos para el uso y el almacenamiento de los datos recopilados; y iv) proporcionen salvaguardias efectivas contra las violaciones[797].

Finalmente propone una reforma al actual sistema de supervisión de las actividades de vigilancia para garantizar su eficacia, entre otras cosas disponiendo la intervención judicial en la autorización o supervisión de las medidas de vigilancia, y considerando la posibilidad de establecer mandatos de supervisión consistentes e independientes con el fin de evitar abusos, absteniéndose de imponer la retención obligatoria de datos por terceros y asegurando que las personas afectadas tengan acceso a recursos efectivos en casos de abuso[798].

En definitiva, podría señalarse que el derecho a la privacidad e intimidad en la sociedad contemporánea supone una serie de desafíos prácticos, requiriendo intensificar el estudio a efectos de que se propongan soluciones relativas a la

---

[797] Comité de Derechos Humanos de la Naciones Unidas, Observaciones finales sobre el cuarto informe periódico de los Estados Unidos de América, 23 de abril de 2014, párr. 22, [en línea], http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsijKy20sgGcLSyqccX0g1nnMFNOUOQBx7X%2BI55yhlwlkDk6CF0OAdiqu2L8SNxDB4%2BTuL0ZaOZ9kVnQN1fWr7Cn3TzJeMcBWzf1aidGZIh9m

[798] Comité de Derechos Humanos, Observaciones finales sobre el cuarto informe periódico de los Estados Unidos de América, 23 de abril de 2014, *op. cit.,* párr. 22.

protección de la ley, garantías procesales, supervisión y recursos efectivos y accesibles para que puedan interponerse en casos de arbitrariedades o ilicitudes.

Si bien el Derecho Internacional de Derecho Humanos, regula y proporciona una protección adecuada del derecho a la privacidad, la interceptación de comunicaciones y la protección de datos personales, lo cierto es que las prácticas de algunos Estados han hecho evidente la falta de protección a través de normas adecuadas y la falta de garantías procesales y de supervisión, máxime que la falta de estos mecanismos ha facilitado a los gobiernos las invasiones a la privacidad de las personas.

4. DESPUÉS DE LAS REVELACIONES DE SNOWDEN.

4.1. The USA Freedom Act (La Ley de Libertad de los EE.UU.).

Los líderes de las agencias de inteligencia y el Presidente de los EE.UU. han manifestado que la vigilancia realizada está justificada en la persecución del terrorismo y la seguridad nacional[799]. Esta misma justificación ha sido utilizada en el pasado[800], tanto para mantener los poderes del Gobierno como para tranquilizar a las personas.

En efecto, gran parte de la vigilancia masiva ha sido útil al gobierno de los Estados Unidos para defenderse de posibles ataques y mantener en firme la seguridad nacional, en especial por tratarse de un país que ha asumido funciones rectoras en diversas partes del planeta, participando en conflictos armados contra grupos o estados totalitarios y no democráticos, combatiendo el narcotráfico y otras formas de criminalidad global, como recientemente ocurrió con el tema de la FIFA.

No obstante, con la vigilancia masiva también se han producido excesos, usos no autorizados y violaciones a los derechos fundamentales, en especial la intimidad y la privacidad.

---

[799] El Presidente de los EE.UU. Barack Obama dijo: "*This is a matter of national security (…) We shouldn't surrender the tools that help keep us safe. It would be irresponsible. It would be reckless"*. Este es un asunto de seguridad nacional, no debemos renunciar a las herramientas que ayudan a mantenernos seguros. Sería irresponsable. Sería imprudente. [traducción libre del autor], YUHAS, A., "NSA surveillance: Obama warns Congress against 'reckless' decision" en *The Guardian,* 30 de mayo de 2015, [en línea], http://www.theguardian.com/us-news/2015/may/30/nsa-surveillance-obama-congress-usa-freedom-act

[800] *Vid. Supra* Cap. VI.2.1.

Esta primera conclusión se toma con base en los documentos revelados por Snowden, los cuales evidencian que la actividad de espionaje ha incursionado en la política y economía interna e internacional, situación que se expuso en el apartado anterior *supra*, pues estos actos de vigilancia no tienen ninguna relación con la persecución del terrorismo, con la defensa de la nación, ni con la persecución de la criminalidad. Es necesario que se recuerde que muchos de los documentos expuesto por Snowden han puesto en evidencia la aplicación del artículo 215 de la Ley Patriota de EE. UU. (USA Patriot Act) contra los a los derechos humanos en EE. UU., al señalar que, al amparo de esta norma, las agencias de inteligencia han recabado registros telefónicos privados de millones de personas en EE. UU. que no tienen vínculos con la delincuencia ni el terrorismo.

La justificación de los gobiernos para la utilización de programas de vigilancia masiva es el mantener la seguridad nacional, principalmente como herramienta contra el terrorismo. Podría ser la seguridad nacional un objetivo legítimo para la restricción del derecho a la privacidad. En ese sentido, debe señalarse que si bien las tecnologías pueden ser y han sido utilizadas por algunas personas con fines delictivos, incluidos actos terroristas, la vigilancia de las comunicaciones electrónicas podría ser útil como medida para que las autoridades o fuerzas de inteligencia puedan hacer frente ante las ilicitudes y puedan hacer cumplir la leyes nacionales e internacionales. Sin embargo, la desproporcionalidad de la medida pareciera anteponerse a la necesidad, a fin de lograr ese objetivo y el beneficio que se obtiene. En ese sentido, si bien pueden utilizarse herramientas tecnológicas para perseguir objetivos legítimos como la seguridad nacional, lo cierto es que el exceso podría hacer que la medida sea arbitraria e ilegítima en el plano de los derechos humanos, los cuales solo deben ceder de forma excepcional.

Tal y como se expuso, la Ley Patriota de los EE.UU., fue aprobada como una respuesta de los ataques del 11 de septiembre de 2001, en la cual el Congreso de los EE.UU. incorpora una cláusula de limitación temporal, a fin de asegurar la caducidad de algunos artículos, incluido el art. 215. La finalidad de esta limitación

era, precisamente, garantizar que la norma fuera reconsiderada una vez que pudieran apreciarse mejor sus consecuencias en términos de derechos.

Dos organismos independientes[801] fueron consultados por parte del Gobierno de los EE.UU. a fin de que rindieran un informe completo sobre las actividades de vigilancia masiva como herramienta utilizada por las agencias de inteligencia para combatir el terrorismo, con base en la facultad que permite el art. 2015 de la Ley Patriota. Los informes fueron concluyentes al señalar que el programa de registros telefónicos no ha significado un aporte para combatir amenazas terroristas, y han instado a que se ponga fin al programa[802].

Entre las principales recomendaciones señaladas por *Liberty and Security in a Changing World* y *Privacy and Civil Liberties Oversight Board* (PCLOB)[*803*] se destacan la necesidad de desarrollar principios que sirvan de base para que en el futuro se respete la libertad y seguridad en un mundo cambiante, reconoce la necesidad de mantener la confianza pública y propone medidas para reducir el riesgo de las divulgaciones no autorizadas. Además, las recomendaciones hacen hincapié en la gestión del riesgo y la necesidad de equilibrar una amplia gama de posibles consecuencias, incluyendo tanto los costes y los beneficios, en la consideración de las reformas posibles.

Puntualmente, señalan los informes:

---

[801] Los organismos independientes consultados fueron: Liberty and Security in a Changing World y Privacy and Civil Liberties Oversight Board (PCLOB).

[802] El reporte completo de Liberty and Security in a Changing World de 12 de diciembre de 2013, puede ser consultado en: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; y el reporte completo de Privacy and Civil Liberties Oversight Board de 23 de enero de 2014 puede ser consultado en: https://www.justsecurity.org/wp-content/uploads/2014/01/Final-Report-1-23-14.pdf

[803] *Ibíd.*

- **Limitar la colección de datos a granel:** Los informes apoyan reformas legislativas para poner fin al almacenamiento de la telefonía mayor (metadatos) por el gobierno, bajo la Sección 215 de la Ley de Vigilancia de Inteligencia Extranjera.
- **Aumentar la transparencia:** Los informes instan al Congreso a promulgar una legislación que autorice a revelar al público información general acerca de las órdenes que reciben los proveedores de teléfono, Internet y otros, en la cual el gobierno solicita información. Además, el gobierno debe dar a conocer de manera pública y con regularidad datos generales acerca de los pedidos que haya emitido en los programas cuya existencia esta sin clasificar.
- **Mejorar la privacidad de personas no estadounidenses:** Los informes establecen varias medidas que debe tomar el gobierno para proteger la privacidad de las personas no estadounidenses, de manera que se extiendan las protecciones de las leyes de privacidad a las personas no estadounidenses.
- **Realizar una reforma organizacional:** Los informes recomiendan una serie de cambios en la organización. Entre los más importante, se recomienda que el Presidente cree un nuevo proceso para aprobar las actividades de inteligencia sensibles, incluidos los procesos políticos de política económica. Crear dentro del Tribunal de Vigilancia de Inteligencia Extranjera el cargo de un Abogado de Interés Público, para que represente los intereses de la privacidad y libertades civiles y cambiar el proceso mediante el cual se nombra a los jueces de este Tribunal. La renovación de la Junta de Privacidad y Libertades Civiles con autoridad para revisar las actividades del gobierno en relación con la inteligencia extranjera. Con respecto a la NSA se propone que el cargo sea aprobado por el Congreso y que se deslinden las funciones para que el puesto del Comando Cibernético sea ocupado por una persona distinta.

- **Crear tecnologías de encriptación:** En relación con la tecnología global de comunicaciones los informes recomiendan que el gobierno apoye las iniciativas para crear fuertes estándares de encriptación a nivel global y tomen las medidas para impulsar el desarrollo, la seguridad, y apertura en Internet.
- **Prevenir riesgos y amenazas internas:** Los informes recomiendan una serie de medidas para reducir los riesgos asociados con estas. Señalan la necesidad de cambiar tanto al personal de investigación con antecedentes y seguridad de la red considerados como "amenazas internas".

Muchas de estas recomendaciones y las revelaciones de Snowden, sobre la vigilancia digital por parte de la NSA, ha generado una serie de reacciones, entre estas la reforma de leyes que han permitido la actividad de las agencias de inteligencia relacionadas con la vigilancia masiva. El pasado 2 de junio se aprobó la ley denominada "USA Freedom Act of 2015"[804], que en esencia limita las competencias de las Agencias del Gobierno Federal de los EE.UU. para fortalecer el respeto del derecho a la privacidad y las libertades civiles. De esta manera prohíbe la vigilancia electrónica de forma masiva, a gran escala, de manera indiscriminada, al igual que la recogida de datos de todo un Estado, ciudad o código postal, con algunos matices y sin que se aplique a todos los programas de vigilancia utilizados.

Como se señaló, esta normativa limita los poderes de las agencias gubernamentales, principalmente en relación a los datos recogidos a gran escala

[804] USA FREEDOM Act of 2015, H.R. 2048, the "**U**niting and **S**trengthening **A**merica by **F**ulfilling **R**ights and **E**nsuring **E**ffective **D**iscipline **O**ver **M**onitoring Act of 2015", [en línea], https://www.congress.gov/bill/114th-congress/house-bill/2048/text; El acrónimo de la ley son las primeras letras de cada una de las palabras del nombre, resaltadas en esta cita. La traducción al español es Ley de Libertad de Estados Unidos de América.

de los registros telefónicos, los llamados metadatos. Entre lo más importante de la reforma, se creó una unidad conformada por un Abogado Defensor del Interés Público que actuará ante el Tribunal creado por la ley FISA, cuya función será supervisar los programas de vigilancia y tiene entre sus facultades la de informar al Congreso de los EE.UU. cuando el Tribunal haga una interpretación de esta ley.

Esta Ley se compone de ocho títulos. El Título I se refiere a la prohibición del Gobierno para utilizar el sistema de recolección de datos en forma masiva permitido hasta entonces bajo la Sección 215. Ahora, en su lugar, se requiere que el Gobierno base o fundamente cualquier solicitud de registro de llamadas en un mandato específico de selección temporal, que identifique a una persona, cuenta, dirección o un dispositivo personal de manera que limite, en mayor medida y de forma razonable y práctica, el alcance de las órdenes requeridas.

El gobierno puede solicitar los registros en una primera oportunidad si: 1. Señala motivos razonables para creer que los detalles del registro de llamadas podrían servir como base de una investigación, y 2. Si tiene una sospecha razonable que lo requerido se asocia con una potencia extranjera, actos o planeamientos terroristas. Para solicitar registros en una segunda instancia, el Gobierno debe señalar la información específica, sea número de identificación o número de tarjera de llamada obtenida en la primera oportunidad.

Para limitar la recolección excesiva, la Ley obliga al Gobierno a adoptar procedimientos de minimización, tales como la destrucción inmediata de todos los registros detallados de llamadas que no sean clasificados como información de inteligencia extranjera. También los jueces de la corte FISA pueden imponer o solicitar de forma adicional este tipo de procedimientos de minimización con respecto a cualquier información disponible de un ciudadano estadounidense.

El Título II de la Ley es breve y se refiere a las leyes Pen/Trap sobre la información de enrutamiento y transmisión de llamadas telefónicas y otras formas de contenido electrónico, como las direcciones IP o los encabezados de los correos

electrónicos. En forma similar a la del Título I prohíbe la recolección de registros comerciales de forma masiva, excepto a través de la solicitud con base en un mandato específico de selección temporal.

El Título III prohíbe utilizar la información de cualquier ciudadano estadounidense obtenida con base en la Sección 702, a través de procedimientos autorizados por el Tribunal de Vigilancia Extranjera FISA, en procesos judiciales. Tampoco puede el Gobierno utilizar o divulgar dicha información de cualquier otra manera.

El Título IV versa sobre la reforma del Tribunal de Vigilancia Extranjera FISA de forma general, se prevé el nombramiento de un *amicus curiae* (curadores o peritos) para asistir al Tribunal de la FISA, sin embargo, los *amicus curiae* son elegidos por el Tribunal de forma discrecional y no de forma objetiva, como por ejemplo a través de concurso o lista de curadores o peritos, situación que limita la participación de los expertos. Otra cuestión que se expone en este Título son las formas de apelación o revisión de las sentencias, las cuales son limitadas. Por último, la desclasificación de las sentencias del Tribunal de Vigilancia Extranjera es necesaria para que ciertas partes de estas resoluciones puedan ser expuestas al público.

En el Título V se introducen reformas al programa Carta de Seguridad Nacional, ampliando las prohibiciones para la colección de datos al igual que en el Título I, exigiendo un mandato específico de selección temporal.

El Título VI establece amplios requisitos para la divulgación de los datos colectados por la Ley FISA. Bajo las secciones 601 y 602, el Gobierno debe poner en conocimiento del Congreso y al público el número de órdenes y certificaciones solicitadas y recibidas, el número de personas afectadas por la vigilancia y el número de personas que han sido catalogadas como objetivo. Bajo la sección 603 se permite a las empresas sujetas a las órdenes informar públicamente sobre la cantidad de órdenes y el tipo de órdenes que ha recibido.

En el Título VII se crea una excepción de emergencia que permite que el Gobierno continúe centrándose en las personas extranjeras fuera de los EE.UU. como objetivos. Además, se amplía el concepto de "agente de una potencia extranjera" con el fin de incluir a las personas de EE.UU. que no son objetivos legítimos bajo las órdenes tradicionales de la FISA, esta ampliación del concepto incluye también a las personas que se dedican a la producción de armas de destrucción masiva fuera de los EE.UU. En este apartado se expande de forma moderada las posibilidades de la Ley en relación con las personas extranjeras.

El Título VIII se refiere a las obligaciones internacionales de los EE.UU. en los asuntos relativos a la seguridad marítima y el terrorismo nuclear. Finalmente, de conformidad con lo señalado en la Sección 705 de la Ley, el período de vigencia es hasta el 2019.

Sobre la aprobación de esta importante la reforma legislativa, Cynthia Wong señaló que *"la Ley de Libertad marca un posible cambio de rumbo en la vigilancia de masas en EE.UU."*, sin embargo, *"las reformas de la ley suponen sólo un modesto primer paso, es la primera vez que el Congreso ha restringido la actividad de la NSA desde los atentados del 11 de septiembre, en 2001."* También apuntó la experta que, *"el Congreso debe tomar medidas para proteger la privacidad de las personas fuera de EE.UU."* [805]

Ciertamente, la reforma aborda solo una pequeña parte de los sistemas de vigilancia de masas de la NSA, que fueron revelados por primera vez por Snowden hace dos años, puesto que no limita la vigilancia bajo la Sección 702 de la Ley de Enmiendas de FISA ni la Orden Ejecutiva 12333. Tampoco se hace referencia en esta reforma a la utilización de todas las capacidades modernas de vigilancia, como

[805] WONG, C., "EE.UU.: Un paso modesto para frenar los excesos del espionaje" *en Human Rights Watch,* 3 de junio de 2015, [en línea], https://www.hrw.org/es/news/2015/06/03/eeuu-un-paso-modesto-para-frenar-los-excesos-del-espionaje

el uso de software malicioso, la interceptación de todas las llamadas vía celular en un país o, la puesta en peligro de la seguridad de equipos y servicios de comunicaciones.

4.2. Sentencia del Tribunal de Justicia Europeo del 6 de octubre de 2015.

En el marco de la protección de datos de la UE, el pasado 6 de octubre de 2015[806], el Tribunal de Justicia declaró inválida la Decisión de la Comisión de las Comunidades Europeas[807] que se declaró que los EE.UU.[808] garantiza un nivel de protección adecuado de los datos personales. Para esta investigación la mencionada sentencia tiene mucha importancia, pues se trata de un pronunciamiento del TJUE sobre el tratamiento de los datos personales, la tutela del derecho de intimidad y la vida privada de las personas en los EE.UU., lo anterior

---

[806] Tribunal de Justicia de la Unión Europea, sentencia en el asunto C-362/14, Luxemburgo, 6 de octubre de 2015, [en línea], http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=240406

[807] Decisión 2000/520/CE de la Comisión de las Comunidades Europeas de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada, [en línea], http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/B.12-cp--Decisi-oo-n--sobre-la-adecuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf

[808] Hasta la fecha, según la Agencia Española de Protección de Datos, además de los EE.UU. los países declarados con un nivel adecuado de protección de datos son los siguientes:

- Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.
- Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.
- Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.
- Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
- Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.
- Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.
- Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
- Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.
- Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
- Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
- Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.

con posterioridad a las denuncias realizadas por Edward Snowden sobre la vigilancia masiva.

Desde 1999 los EE.UU. realizaron negociaciones en orden a conseguir una declaración de adecuación del nivel de protección de datos personales. Normalmente se analiza la legislación y prácticas de un país con respecto al tratamiento de estos datos a fin de evaluar si tiene o no un nivel adecuado. En el caso de los EE.UU. no existe una normativa sobre protección de datos de carácter personal en todo el territorio, que abarque todos los sectores de la actividad, por el contrario, existe una normativa dispersa y específica en sectores concretos[809]. Por lo anterior, el Departamento de Comercio de los EE.UU. presentó como documento para discusión un borrador de "principios de puerto seguro", al cual debían someterse los operadores manifestando su adhesión y compromiso.

El Acuerdo de Puerto Seguro consta de siete principios[810], notificación, opción, transferencia ulterior a terceras empresas, seguridad, integridad de los datos, derecho de acceso y aplicación. Estos principios se complementan con las *Frequently Asked Questions* FAQs (preguntas más frecuentes).

Con respecto a los hechos que permitieron el comentado pronunciamiento del TJUE, estos iniciaron con el caso planteado por el señor Maximillian Schrems, ciudadano austriaco, que en su condición de usuario de Facebook alegaba que sus datos se transferían total o parcialmente de la filial irlandesa de esta red social a los

---

[809] *Vid.* *Supra* Cap. III, apartado 2.1.4.3.

[810] En la página oficial http://export.gov/safeharbor/index.asp se pueden consultar las regulaciones generales de las organizaciones asociadas a los principios de puerto seguro. Los principios de puesto seguro se pueden ser consultados en línea en: http://www.export.gov/safeharbor/eu/eg_main_018476.asp

servidores situados en los EE.UU., lugar en el cual eran objeto de tratamiento. Luego de las revelaciones de Edward Snowden en el 2013, el señor Schrems presentó una denuncia ante la autoridad irlandesa de control, por estimar que la normativa y las prácticas de los EE.UU. no eran garantía suficiente de los datos transferidos[811] a ese país, principalmente a raíz de las actividades de inteligencia y vigilancia masiva llevadas a cabo por parte de la NSA. En esa primera instancia, la autoridad irlandesa desestimó esa reclamación con fundamento en la Decisión de la Comisión de 26 de julio de 2000 en la cual EE.UU. fue considerado como "puerto seguro" al valorarse su normativa y prácticas con un nivel adecuado de protección de los datos transferidos.

La negativa de parte de la autoridad irlandesa, permite al accionante acudir a la *High Court* de Irlanda (Tribunal Supremo irlandés), que constató que el Derecho irlandés prohíbe la transferencia de datos personales fuera del territorio nacional, excepto cuando el tercer país interesado asegura un nivel de protección adecuado de la vida privada y de los derechos y libertades fundamentales, también, la Constitución irlandesa resalta los derechos al respeto de la vida privada y a la inviolabilidad del domicilio, así como, exige que toda injerencia en esos derechos sea proporcionada y ajustada a las exigencias previstas por la ley. Adicionalmente, la *High Court* irlandesa estimó que *"**el acceso masivo e indiferenciado a los datos personales es manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales protegidos por la Constitución irlandesa**. Para que las interceptaciones de comunicaciones electrónicas puedan ser consideradas*

[811] Según se define en el artículo 5.1.s. del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado mediante Real Decreto 1720/2007, la Transferencia internacional de datos es el tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

conformes con esa Constitución, debe aportarse la ***prueba de que esas interceptaciones tienen carácter selectivo, de que la vigilancia de determinadas personas o de determinados grupos de personas está objetivamente justificada en interés de la seguridad nacional o de la represión de la delincuencia y de que existen garantías adecuadas y comprobables****".*[812]

Dado que la *High Court* de Irlanda, estimó que "*si el asunto principal se tuviera que resolver con fundamento exclusivo en el Derecho irlandés, se debería apreciar que, dada la existencia de serias dudas de que Estados Unidos garantice un nivel adecuado de protección de los datos personales, el comisario* [primera instancia] *habría debido llevar a cabo una investigación sobre los hechos denunciados por el Sr. Schrems en su reclamación, y que la desestimó indebidamente*".[813] Esto motivó a que el caso planteado fuese admitido para el estudio, sin embargo, al estar determinado el fondo del asunto a resolver si el Comisario estaba vinculado por la constatación realizada por la Comisión en la Decisión 2000/520/CE, según la cual Estados Unidos garantiza un nivel de protección adecuado, o bien si en virtud de lo expuesto en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, se autorizaba al Comisario a separarse de esa constatación para poder atender la denuncia y haber realizado una investigación, situación que finalmente motivó la suspensión del proceso y plantear la cuestión prejudicial ante el TJUE para que conociera del asunto y se pronunciara sobre si la Decisión de la Comisión de las Comunidades Europeas de 26 de julio de 2000, impedía a las autoridades de control pronunciarse o investigar ante una denuncia en la cual se acuse que terceros países no cumplen con un nivel adecuado y se pueda suspender la transferencia de datos.

---

[812] *Vid.* Tribunal de Justicia de la Unión Europea, sentencia en el asunto C-362/14, Luxemburgo, 6 de octubre de 2015, aparatado 33.

[813] *Ibíd.*

Debe advertirse que la valoración realizada por parte de la Comisión de las Comunidades Europeas fue tomada en el año 2000 y, en esa oportunidad se estimó que EE.UU. cumplía con el principio de “puerto seguro” para la transferencia de archivos, esto muchos años antes de las denuncias del año 2013.

El Tribunal Supremo irlandés eleva la consulta ante el TJUE, situación que permite el pronunciamiento del máximo tribunal de justicia europeo. Debe entenderse que este pronunciamiento se refiere a la vigencia de la Decisión 2000/520/CE de la Comisión con respecto al nivel de protección de datos personales que ofrece un país tercero, mandamiento que emana de la directiva 95/46 sobre la protección de las personas frente al tratamiento de sus datos personales, particularmente lo dispuesto en su artículo 25. En ese sentido, si un país no garantiza un nivel de protección adecuado, los Estados miembros pueden adoptar las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país que se trate, en el caso concreto los EE.UU.

Concretamente, la *High Court* de Irlanda planteó ante el TJUE:

1. En el marco de la resolución de una reclamación presentada ante el comisario, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, Estados Unidos) cuya legislación y práctica no prevén una protección adecuada de la persona sobre la que versan los datos, ¿está vinculado dicho comisario en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión 2000/520, habida cuenta de los artículos 7, 8 y 47 de la Carta y no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE?
2. En caso contrario, ¿puede o debe realizar dicho comisario su propia investigación del asunto a la luz de la evolución de los hechos que ha

tenido lugar desde que se publicó por vez primera la Decisión 2000/520?[814]

Sobre el primer planteamiento, el TJUE estimó que las autoridades nacionales de control gozan de una garantía de independencia, lo que les permite asegurar un control eficaz y fiable en materia de transferencia de datos personales a terceros países, según se dispone en el artículo 28.1 de la Directiva 95/46, garantía que se entiende como una exigencia a los Estados Miembros. Esta exigencia también deriva del artículo 8. 3, de la Carta de los Derechos Fundamentales de la Unión Europea y del artículo 16 del Tratado de Funcionamiento de la Unión Europea[815].

De esta manera puede interpretarse que, aunque exista una Decisión de la Comisión sobre el nivel de garantía de protección de un tercer país, esto no impide a las autoridades nacionales de control el examen de la solicitud planteada por una persona sobre la protección de los datos personas que pudiesen ser enviados a un tercer país. Por el contrario, el artículo 28 de la Directiva 95/46 se aplica por su propia naturaleza a todo tratamiento de datos personales, incluyendo la transferencia de datos, las que de conformidad con lo indicado por el TJUE pueden ser investigadas con toda independencia por parte de las autoridades nacionales de

---

[814] *Vid.* Tribunal de Justicia de la Unión Europea, sentencia en el asunto C-362/14, Luxemburgo, 6 de octubre de 2015, apartado 36.

[815] De esta forma, según señaló el TJUE *"… las autoridades nacionales de control disponen de una amplia gama de facultades, y éstas, enumeradas de forma no exhaustiva por el artículo 28, apartado 3, de la Directiva 95/46, constituyen otros tantos medios necesarios para el cumplimiento de sus funciones, como destaca el considerando 63 de esa Directiva. Así pues, esas autoridades disponen, en particular, de facultades de investigación, como la de recabar toda la información necesaria para el cumplimiento de su misión de control, de facultades efectivas de intervención, como la de prohibir provisional o definitivamente un tratamiento de datos, o la capacidad de comparecer en juicio"*. Tribunal de Justicia de la Unión Europea, sentencia en el asunto C-362/14, Luxemburgo, 6 de octubre de 2015, apartado 43.

control para determinar si se cumplen o no las exigencias indicadas en la Directiva 95/46.

Con respecto a la posibilidad y legitimidad que tienen las autoridades nacionales de control con respecto a la protección de las personas sobre el tratamiento de sus datos personales y pese a las Decisiones de la Comisión, termina por concluir, sobre este aspecto, el TJUE que *"…el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de los artículos 7, 8 y 47 de la Carta* [Carta de los Derechos Fundamentales de la Unión Europea]*, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado."* [816]

Con relación a la validez de la Decisión 2000/520/CE de la Comisión el TJUE valoró, la sentencia de comentario señala que, un nivel de protección adecuado se refiere a la garantía de un tercer País "a la vista de su legislación interna o de sus compromisos internacionales", pues la fiabilidad de ese sistema en relación con dicha exigencia descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica

[816] Tribunal de Justicia de la Unión Europea, sentencia en el asunto C-362/14, Luxemburgo, 6 de octubre de 2015, apartado 66.

las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales[817].

Adicionalmente, se aclara en el referido fallo que los principios de puerto seguro le son aplicables únicamente, a las entidades autocertificadas que reciben los datos personales de la UE, requisito no exigible a las autoridades públicas estadounidenses.

En la Decisión 2000/520/CE de la Comisión se reconocen las exigencias de los EE.UU. con respecto a la seguridad nacional, el interés público y el cumplimiento de la ley, razón por la cual las autoridades estadounidenses autocertificadas que reciban datos personales de la UE están obligadas a dejas de aplicar los principios de puerto seguro cuando estos entren en conflicto con la seguridad nacional, el interés público y el cumplimiento de la ley[818].

También resalta el TJUE en la sentencia de comentario que en la Decisión 2000/520/CE de la Comisión no se indican los mecanismos eficaces contra las injerencias en la protección de los datos de las personas transferidos a los EE.UU. desde la UE. por lo cual no se pueden realizar litigios sobre la legalidad de las

---

[817] *Ibíd.,* apartado 81.

[818] Tribunal de Justicia de la Unión Europea, sentencia en el asunto C-362/14, Luxemburgo, 6 de octubre de 2015, apartado 86. Por esta razón, la excepción prevista en el anexo I de la citada Decisión permite las injerencias en la vida privada de las personas, fundadas en exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de los EE.UU., con la posible vulneración de los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse desde la UE a los EE.UU. De otra parte, tampoco existe algún medio de constatación de las exigencias que posibilitan tal injerencia en los datos personales transferidos.

injerencias en los derechos fundamentales derivadas de las medidas de origen estatal[819].

Como bien lo señala el TJUE, la propia Comisión en la Comunicación COM(2013) 846 final y la Comunicación COM(2013) 847 final ya había advertido que, *"…las autoridades estadounidenses podían acceder a los datos personales transferidos a partir de los Estados miembros a Estados Unidos y tratarlos de manera incompatible con las finalidades de esa transferencia, que va más allá de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional"*.[820]

Tal y como se advirtió *supra* en el apartado de esta Capítulo 3.3, las limitaciones de las libertades y derechos fundamentales, según también la reiterada Jurisprudencia del TJUE[821] cualquier limitación de los derechos fundamentales garantizados por los artículos 7 y 8 del TFUE debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas que resulten afectadas puedan dispongan de las garantías suficientes que permitan proteger sus derechos contra cualquier amenaza o vulneración de sus derechos.[822]

---

[819] *Ibíd.,* apartados 88 y 89.

[820] Tribunal de Justicia de la Unión Europea, sentencia en el asunto C-362/14, Luxemburgo, 6 de octubre de 2015, apartado 90.

[821] *Vid.* Sentencias Les Verts/Parlamento, 294/83, apartado 23; Johnston, 222/84, apartados 18 y 19; Heylens y otros, 222/86, apartado 14, y UGT-Rioja y otros, C-428/06 a C-434/06, apartado 80, todas del Tribunal de Justicia de la Unión Europea.

[822] *Ibíd.,* apartados 91-93. Debe recordarse que la protección del derecho fundamental al respeto de la vida privada al nivel de la UE exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario. Situación que no se cumple en el caso de las normas que permiten la conservación de los datos de forma generalizada, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin

El TJUE ha sido claro al señalar que "la normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta [Carta de los Derechos Fundamentales de la Unión Europea]", así como la "normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta [Carta de los Derechos Fundamentales de la Unión Europea]"[823]. Es decir, si se carece por completo de un mecanismo efectivo para la tutela de los derechos de las personas, se vulneran de forma grosera sus derechos, lo cual no es compatible con un Estado de Derecho.

Finalmente el TJUE en la sentencia de comentario señala que no es preciso pronunciarse a los principios de puerto seguro en el caso concreto pues en la Decisión 2000/520/CE la Comisión no se pronuncia sobre el nivel de protección de los EE.UU. en razón de su legislación interna o sus compromisos internacionales. De esta manera, concluye que en virtud de la normativa europea analizadas no se inhibe a las agencias controladoras nacionales para investigar sobre el cumplimiento de requisitos en la transferencia de datos personales a un tercer país por el hecho de que exista un pronunciamiento de puerto seguro para ese país. Así

---

prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización.

[823] Tribunal de Justicia de la Unión Europea, sentencia en el asunto C-362/14, Luxemburgo, 6 de octubre de 2015, apartados 93-95.

mismo, al estimarse que los artículos 1 y 3 de la Decisión son inválidos e indisociables con el 2 y 4 determina que esta, en su totalidad, es inválida.

Tras la declaratoria de invalidez de la Decisión 2000/520/CE, las agencias de protección de datos de la UE publicaron una declaración conjunta en la cual señalaron que las transferencias basadas en el acuerdo de puesto seguro eran ilegales[824]. Las Autoridades de protección de datos de los Estados miembros de la UE, reunidas en el Grupo de Trabajo del Artículo 29 hicieron un llamado a los Estados miembros y a las Instituciones europeas para encontrar soluciones políticas, jurídicas y técnicas que permitan transferencias de datos a EEUU respetando los derechos fundamentales.

El Grupo de Trabajo del Artículo 29 señaló que si bien no podrían transferirse datos de las empresas basadas en el acuerdo de puerto seguro se podría continuar con dichas transferencias basadas en las Cláusulas Contractuales Tipo y las Normas Corporativas Vinculantes (BCRs).

El panorama de la transferencia de datos entre la UE y los EE.UU. aún no es claro, sin embargo, se puede inferir la necesidad de un pronto y nuevo acuerdo de Puerto Seguro que ofrezca los mecanismos de defensa claros y vinculantes e incluya la supervisión del acceso por parte de las autoridades públicas, principalmente en lo que respecta a la transparencia, proporcionalidad, mecanismos de reparación y derechos recogidos en la legislación de protección de datos personales.

---

[824] Notas de prensa de la AEPD, “Las Autoridades europeas de Protección de Datos publican una declaración conjunta en relación con la aplicación de la sentencia del TJUE sobre el Puerto Seguro”, 19 de octubre de 2015, [en línea], http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_19-ides-idphp.php

El Parlamento Europeo requirió a la Comisión a que evalúe pormenorizadamente hasta qué punto interferiría e incidiría exactamente este acuerdo marco en el marco jurídico sobre la protección de datos de la UE en particular en la actual decisión marco del Consejo, la Directiva sobre protección de datos (95/46/CE) y la directiva y el reglamento futuros sobre la protección de datos respectivamente, por ello pidió a la Comisión que presentara un informe de evaluación jurídica al respecto antes de que se inicie el procedimiento de ratificación[825].

Particularmente, también en la citada resolución[826] el Parlamento Europeo solicitó a los Estados miembros de la UE que retiren los cargos penales que hubiere contra Edward Snowden y le ofrezcan protección e impidan, por lo tanto, su extradición o entrega por terceras partes, en reconocimiento de su condición de denunciante de irregularidades y defensor de los derechos humanos internacionales.

También el Parlamento Europeo considera que siguen peligrando los derechos fundamentales de los ciudadanos de la UE y que no se ha hecho lo suficiente para asegurar su plena protección en caso de vigilancia electrónica masiva, lamenta los escasos avances a la hora de garantizar la protección de los denunciantes de irregularidades y los periodistas. Asimismo, señaló programas de inteligencia masiva y a gran escala parecen estar manejados por los intereses económicos de las empresas que desarrollan y ejecutan dichos programas, como

---

[825] Resolución del Parlamento Europeo, de 29 de octubre de 2015, sobre el seguimiento de la Resolución del Parlamento Europeo, de 12 de marzo de 2014, relativa a la vigilancia electrónica masiva de los ciudadanos de la UE (2015/2635(RSP)).

[826] *Ibíd.* Acuerdo 5.

fue el caso que condujo a la finalización del programa “ThinThread”[827], dirigido por la NSA, y su sustitución por el programa de vigilancia a gran escala “Trailblazer”, que se subcontrató a SAIC en 2001.

[827] ThinThread es el nombre de un proyecto de la NSA para el análisis de escuchas telefónicas. Este programa fue reemplazado por el programa Trailblazer por el cual se suscribió un contrato por más de 280 millones de dólares en el año 2002. *Cfr.* MCLEAN, V, “SAIC Team Wins National Security Agency TRAILBLAZER Contract” (BUSINESS WIRE), 21 de octubre de 2002, [en línea], http://www.thefreelibrary.com/SAIC+Team+Wins+National+Security+Agency+TRAILBLAZER+Contract.-a093081931

4.3. Hacia una nueva forma de protección de la privacidad.

Tal y como se ha advertido, los derechos a la privacidad e intimidad en la era digital presentan una variedad de importantes desafíos prácticos. Con fundamento en el examen realizado en la presente investigación sobre algunos de estos desafíos, pareciera imperativo que en este momento se intensifique el debate y se realicen más estudios sobre las cuestiones relativas a la protección de los derechos de privacidad e intimidad, de manera que se amplíen los ámbitos de cobertura de la ley, se incluyan más y mejores garantías procesales, se haga una adecuada supervisión y se permita el acceso a recursos efectivos.

Dado que el derecho de intimidad se concibe como un derecho humano necesario para las sociedades democráticas modernas, parte esencial de la dignidad humana que refuerza a su vez otros derechos como la libertad de expresión, el derecho de acceso a la información, la libertad de asociación, el secreto de las comunicaciones y la protección de los datos de las personas, derechos que han sido reconocidos por el Derecho Internacional de los Derechos Humanos, es más que evidente que cualquier restricción o limitación de estos derechos se justifique solo en leyes expresas, redactadas de forma clara, que estas limitaciones se apliquen cuando sea estrictamente necesario para alcanzar un fin mayor, que se dé a través de mecanismos procesales efectivos, sean excepcionales y temporales, además sean proporcionales en cuanto al objetivo perseguido y se dispongan los recursos necesarios para que las personas puedan defender sus derechos en caso de arbitrariedades.

Existe aún la necesidad de que se proporcione a los Estados una mayor orientación práctica, con base y fundamento en el Derecho Internacional de los Derechos Humanos, sobre los principios de necesidad, proporcionalidad y legitimidad en relación con las prácticas de vigilancia, en la cual se incluyan medidas de supervisión efectiva, independientes e imparciales. De otra parte, se necesita

involucrar a las grandes empresas de Internet para que cumplan con un respeto adecuado a los derechos humanos, teniendo en consideración las vulnerabilidades de los datos de las personas ante el uso de tecnologías, e incluyan procedimientos para proteger esos datos ante riesgos o ataques y fomenten la debida gestión de recursos efectivos.

La vigilancia de las comunicaciones en la actualidad se presenta como una actividad desplegada por parte de las agencias de inteligencia mediante la cual pueden monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones hechas o en tiempo real de las personas, actividad que en definitiva no ha sido controlada de forma adecuada y con ello se ha permitido una actuación sin límites, que facilita la posibilidad de actos irregulares y vulneración de los derechos de las personas.

El concepto tradicional de comunicaciones debe ser ampliado de forma tal que incluya, no solo a las formas convencionales, sino también otras actividades, tales como cualquier tipo de interacciones y transacciones transmitidas por medios electrónicos, protegiendo con ello el contenido, la identidad de las partes, información de rastreo de direcciones IP, los datos relacionados con el tiempo y lugar de las comunicaciones, así como otros identificadores de equipos electrónicos, salvo cuando la intercepción y el almacenamiento se justifique, y sea autorizado en forma expresa para perseguir el terrorismo, la delincuencia organizada, el narcotráfico, y otras formas de criminalidad, así como cuando esté comprometida la seguridad nacional, en los términos que indique la ley.

Las tecnologías son tan efectivas que permiten, a pesar que los datos (metadatos) no incluyen el contenido de las comunicaciones, crear perfiles y patrones de las personas de forma más efectiva que el contenido mismo. Lo anterior permite analizar además de forma colectiva datos como la identidad, el comportamiento, las asociaciones, las condiciones físicas o estado de salud, la raza, el color, la orientación sexual, el origen nacional o puntos de vista, o puede permitir el mapeo de la ubicación de las personas, sus movimientos e interacciones en el

tiempo, información que por lo general no se encuentre protegida de forma adecuada.

Varios organismos internacionales[828], organizaciones no gubernamentales[829], grupos de expertos[830] y sectores de la sociedad civil[831] han

---

[828] *Vid.* Informe de la Oficina del Alto Comisionado de Naciones Unidas de Derechos Humanos, del 30 de junio de 2014, sobre el derecho a la privacidad en la era digital, [en línea], http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; Asamblea General, Naciones Unidas, Resolución 68/167, 18 de diciembre de 2013, [en línea], http://www.un.org/es/comun/docs/?symbol=A/RES/68/167

[829] *Vid.* Amnistía Internacional, Campaña dejen de seguirme, [en línea], https://www.amnesty.org/es/get-involved/unfollowme/; Human Rights Watch, "UK: Human Rights Watch Challenges Surveillance", [en línea], https://www.hrw.org/news/2015/09/14/uk-human-rights-watch-challenges-surveillance; Privacy International, consultable en: https://www.privacyinternational.org/; Asociación para el Progreso de las Comunicaciones, consultable en: https://www.apc.org/es/node/93 ; Electronic Frontier Foundation, consultable en: https://www.eff.org/es y Necessary and Proportionate Principles, "International Principles on the Application of Human Rights to Communications Surveillance", [en línea], https://es.necessaryandproportionate.org/

[830] *Vid.* DÍAZ-CANEJA GRECIANO, J. M., "La cooperación de inteligencia en la unión europea", en *Instituto Español de Estudios Estratégicos*, No. 151, 2014; SCHNEIER, B., *Data and Goliath. The hidden battles to collect your data and control your world,* Editorial W.W. Norton & Company, New York, London, 2015, [versión para lector digital Kindle]; SOLOVE, D. J., *Nothing to hide: the false tradeoff between privacy and security,* Yale University Press, New Haven and London, 2013; SOLOVE, D. J. y SCHWARTZ, P. M., Privacy Law Fundamentals, IAPP Publications, 3era edición, New Haven, 2015; HANKIN, R., *Invasion of privacy & the law*, Looseleaf Law Publications, New York, 2013, [versión para lector digital Kindle]; SOMA J. T., RYNERSON, S. D. y KITAEV, E., *Privacy Law*, Editorial West, Minnesota, 2014, [versión para lector digital Kindle]; *v. et.*, El reporte completo de Liberty and Security in a Changing World de 12 de diciembre de 2013, puede ser consultado en: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; y el reporte completo de Privacy and Civil Liberties Oversight Board de 23 de enero de 2014 puede ser consultado en: https://www.justsecurity.org/wp-content/uploads/2014/01/Final-Report-1-23-14.pdf

[831] *Vid.* Bruce Schneier, internationally renowned security technologist, Caspar Bowden, privacy advocate, formerly chief privacy adviser at Microsoft, Danah Boyd, Principal Researcher, Microsoft Research and Research Assistant Professor, New York University, Dr. Ian Brown, Associate Director of Oxford University's Cyber Security Centre, and Senior Research Fellow at the Oxford Internet Institute, Andrew Clement, Professor, Faculty of Information, University of Toronto, Simon Davies, Founder Privacy International. Editor The Privacy Surgeon, Julie E. Cohen, Professor of Law at the Georgetown University Law Center, Michael Geist, Canada Research Chair in Internet and E-commerce Law, University of Ottawa.

propuesto una serie de recomendaciones para proteger los derechos fundamentales de las personas, ante la utilización de programas de vigilancia masiva y la recogida de datos a granel por parte de las agencias de inteligencia y empresas privadas. Para efectos de la presente investigación se pretenden incorporar, analizar, recapitular y ordenar algunas de dichas soluciones, por estimarse indispensables para lograr un posible abordaje al problema planteado en el estudio realizado. Asimismo, se sugieren medios para enfrentar el fenómeno de la vigilancia masiva, teniendo como objetivo el respeto de los derechos fundamentales de las personas.

Entre las principales propuestas y las que han tenido mejor aceptación, se encuentran la realizada por parte de la ONG Necessary and Proportionate[832] que a través de 13 principios resalta la necesidad que los Estados incorporen reglas generales en relación a la utilización de la vigilancia masiva, esta propuesta ha sido firmada por más de 420 organizaciones, 50 expertos, académicos e individuos prominentes, así como 6 miembros importantes de partidos políticos.

De esta manera exponen de forma resumida los siguientes 13 principios[833]:

Principio de Legalidad: Cualquier limitación a los derechos humanos debe ser prescrita por ley, dentro del marco legal, democrático y constitucional. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un

---

[832] Necessary and Proportionate Principles, “International Principles on the Application of Human Rights to Communications Surveillance”, [en línea], https://es.necessaryandproportionate.org/

[833] Estos principios fueron elaborados en octubre de 2012 en una reunión de más de 40 expertos de seguridad y privacidad en Bruselas. Después de una amplia consulta inicial, que incluyó una segunda reunión en Río de Janeiro en diciembre de 2012, Access, EFFy Privacy International condujeron un proceso de redacción colaborativa inspirada en la pericia sobre derechos humanos y derechos digitales de expertos de todo el mundo. La primera versión de los Principios se finalizó el 10 de julio de 2013, y fue lanzada oficialmente en el Consejo de Derechos Humanos de la ONU en Ginebra en setiembre de 2013.

estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Dado el ritmo de los cambios tecnológicos, las leyes que limitan el derecho a la privacidad deben ser objeto de revisión periódica por medio de un proceso legislativo o reglamentario de carácter participativo.

***Principio de objetivo legítimo*:** Las leyes sólo deberían permitir la Vigilancia de las Comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición[834].

Principio de necesidad: Leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La Vigilancia de las Comunicaciones sólo debe llevarse a cabo cuando es el único medio –razonable- para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado[835].

---

[834] Pareciera necesario que se identifiquen de forma taxativa, los objetivos legítimos para intervención de comunicaciones, delimitando de los casos excepcionales para realizar una vigilancia de las comunicaciones de forma masiva o a granel, tales como actividades terroristas, seguridad de la nación o actos delictivos de lesa humanidad.

[835] En relación con este principio debiera señalarse que tanto la necesidad como la idoneidad debiesen ser atendidos de forma razonable, es decir limitar estas actividades de vigilancia a la razonabilidad de la medida, identificando de forma clara el objetivo perseguido, la necesidad, así como la razonabilidad e idoneidad de la medida de intervención a utilizar.

***Principio de idoneidad*:** Cualquier caso de Vigilancia de las Comunicaciones autorizado mediante ley debe ser apropiado –y razonable- para cumplir el objetivo legítimo específico identificado.

***Principio de proporcionalidad*:** La Vigilancia de las Comunicaciones debería ser considerada como un acto altamente intrusivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática. Las decisiones sobre la Vigilancia de las Comunicaciones deben considerar la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses en competencia[836].

Esto requiere que un Estado, como mínimo, debe demostrar ante una autoridad judicial competente y antes de la realización de la Vigilancia de las Comunicaciones que:

- Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo;
- Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la Información Protegida;
- Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica;

[836] Se estima que el principio de proporcionalidad es uno de los más importantes a efecto de solicitar o autorizar alguna medida de vigilancia en las comunicaciones o actividades electrónicas de las personas, debe de ser consecuente con el objetivo principal evaluando la gravedad de la amenaza y la posible vulneración de los derechos de las personas, especialmente el derecho de intimidad y privacidad.

- La información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza específica al fin legitimo alegado;
- Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud;
- La información será accesada solo por la autoridad específica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización;
- Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales[837].

***Principio de autoridad judicial competente*:** Las decisiones relacionadas con la Vigilancia de las Comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente. La autoridad debe:

- Estar separada e independiente de las autoridades encargadas de la Vigilancia de las Comunicaciones;
- Estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la Vigilancia de las Comunicaciones, las tecnologías utilizadas y los derechos humanos, y;

[837] Entre las condiciones para la utilización de la información deberían agregarse el tiempo por el cual tendrá la autoridad la información relevante para su examen, exigiendo la destrucción de esa información una vez que no sea necesaria o transcurrido el plazo. Lo anterior para evitar posibles ataques, la revelación no autorizada o la sustracción de la información colectada.

- Tener los recursos adecuados para el ejercicio de las funciones que se le asignen[838].

***Principio de debido proceso*:** El debido proceso exige que los Estados respeten y garanticen los derechos humanos de las personas, asegurando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público general. En forma específica, al decidir sobre sus derechos, toda persona tiene derecho a una audiencia pública y justa, dentro de un plazo razonable, por un tribunal independiente, competente e imparcial establecido por ley, salvo en casos de emergencia donde exista un riesgo inminente de peligro para la vida humana. En tales casos debe buscarse una autorización con efecto retroactivo, dentro de un plazo razonable y factible. El mero riesgo de fuga o de destrucción de pruebas no se considerará suficiente para justificar la autorización con efecto retroactivo[839].

Principio de notificación del usuario: Aquellos cuyas comunicaciones están siendo vigiladas deben ser notificados de la decisión de autorizar la Vigilancia de Comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los

---

[838] Una cuestión importante sobre la autoridad competente está relacionada con el nombramiento de los jueces que integrarán este tribunal, se estima que, dicho nombramiento no debe recaer en el gobierno central y debe ser, en la medida de lo posible, un nombramiento realizado por parte del congreso para asegurar la independencia y la representación de los diversos sectores de la sociedad.

[839] Mediante el carácter instrumental de este principio, se deberán asegurar todas las garantías propias de un proceso judicial, incluyendo la defensa de intereses generales frente a las solicitudes presentadas por las agencias y organismos que requieran de la información para una investigación concreta. Además, en términos de sensibilidad de la información se deberá agravar el proceso utilizado a fin de que se proteja esa información, dependiendo del grado de sensibilidad y la cantidad de información requerida.

materiales presentados en apoyo de la solicitud de autorización. El retraso en la notificación solo se justifica en las siguientes circunstancias:

- La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana;
- La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia;
- El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente; y
- La obligación de notificar recae en el Estado, pero los proveedores de servicios de comunicaciones deben tener la libertad de notificar a las personas de la Vigilancia de las Comunicaciones, de forma voluntaria o bajo petición[840].

Principio de transparencia: Los Estados deben ser transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, reglamentos, actividades, poderes o autoridades. Deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y propósito, y el número específico de personas afectadas por cada una, y según el tipo de investigación y sus propósitos. Los Estados deben proporcionar a las personas la información suficiente para que puedan comprender plenamente el alcance, la naturaleza y la aplicación de las leyes que permiten la Vigilancia de las

[840] Pareciera razonable que las personas que fueron sometidas a algún tipo de vigilancia, deban ser notificadas una vez que la vigilancia se realizó. Lo anterior a efectos de que puedan hacer valer ciertos derechos o ser indemnizados en caso de que se tratara de una vigilancia arbitraria o ilegal.

Comunicaciones. Los Estados no deberían interferir con los proveedores de servicios en sus esfuerzos para publicar los procedimientos que aplican en la evaluación y el cumplimiento de solicitudes de los Estados para la Vigilancia de Comunicaciones, tampoco cuando se adhieran a esos procedimientos, y pretendan publicar los registros de las solicitudes de los Estados para la Vigilancia de las Comunicaciones[841].

***Principio de supervisión pública*:** Los Estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones.

Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado, incluyendo, según proceda, al acceso a información secreta o clasificada para valorar si el Estado está haciendo un uso legítimo de sus funciones legales, para evaluar si el Estado ha publicado de forma transparente y precisa información sobre el uso y alcance de las técnicas y poderes de la Vigilancia de las Comunicaciones; y para formular determinaciones públicas en cuanto a la legalidad de dichas acciones, incluyendo la medida en que cumplan con estos principios. Mecanismos de supervisión independientes deben establecerse, además de cualquier supervisión ya proporcionada a través de otra rama del gobierno[842].

Principio de integridad de las comunicaciones y sistemas: A fin de garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones,

---

[841] La transparencia no ha sido uno, precisamente, una de las características de las agencias de vigilancia, la mayoría de la información relacionada es catalogada como confidencial, tendiéndose en la práctica pocas posibilidades para contralar la actividad desplegada.

[842] Al igual que con la transparencia, es poco probable que las actividades de vigilancia puedan ser controladas, sin embargo deberían establecerse mecanismos de control y supervisión de las actividades desplegadas por estas agencias, pudiéndose informar al congreso en casos especiales que se determinen mediante una ley.

y en reconocimiento del hecho de que poner en peligro la seguridad con fines estatales casi siempre afecta la seguridad en términos generales, los Estados no deben obligar a los proveedores de servicios o proveedores de “hardware” o “software” a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado. La retención o la recopilación de datos a priori nunca debe ser exigida a los proveedores de servicios. Las personas tienen el derecho a expresarse anónimamente, por lo que los Estados deben abstenerse de obligar a la identificación de los usuarios[843].

Principio de garantías para la cooperación internacional: En respuesta a los cambios en los flujos de información y en las tecnologías y servicios de comunicaciones, los Estados pueden necesitar procurar la asistencia de un proveedor de servicios extranjero y otros Estados. En consecuencia, los tratados de asistencia judicial recíproca (MLAT, por sus siglas en inglés) y otros acuerdos celebrados por los Estados deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la Vigilancia de las Comunicaciones, se adopte la norma estándar disponible con el mayor nivel de protección para las personas. El principio de la doble incriminación debe ser aplicado en el momento en que los Estados procuren asistencia para efectos de hacer cumplir su legislación interna. Los Estados no pueden utilizar los procesos de asistencia judicial recíproca y las solicitudes extranjeras de Información Protegida para burlar las restricciones del

[843] Los desarrolladores de hardware y software, deberían poder garantizar a los usuarios sistemas de protección de desde el origen y por defecto para garantizar la privacidad de los usuarios. Las posibilidades de incluir en los aparatos o programas dispositivos que permiten la recogida de datos o rastreo de personas debería estar prohibida, incluso a las autoridades de gobierno, pues la implementación de esos sistemas pone en riesgo a los usuarios, quienes podrían además ser víctimas de otras personas que aprovechen las tecnologías implantadas por los gobiernos en todos los dispositivos o programas.

derecho interno relativas a la Vigilancia de las Comunicaciones. Los procesos de asistencia judicial recíproca y otros acuerdos deben estar claramente documentados, a disposición del público y sujetos a las garantías de equidad procesal[844].

Principio de garantías contra el acceso ilegítimo y derecho a recurso efectivo: Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegales por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los "*whistle blowers*" y medios de reparación a las personas afectadas. Las leyes deben estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier prueba derivada de dicha información. Los Estados también deben promulgar leyes que establezcan que, después de que el material obtenido, a través de la Vigilancia de las Comunicaciones, ha sido utilizado con la finalidad por el que fue obtenida la información, el material no debe ser retenido, en su lugar debe ser destruido o devuelto a los afectados[845].

---

[844] La cooperación internacional en materia de espionaje ha sido utilizada desde antes de finalizar la Segunda Guerra Mundial, a través de tratados y convenios, en la mayoría secretos, con el propósito de compartir información sobre amenazas y enemigos comunes. Sin embargo, en la práctica no se establecen garantías sobre las posibilidades que tienen los Estados para vigilar a los extranjeros, incluso de países aliados. Además, como se evidenció con las revelaciones de Snowden, se han realizado vigilancias con fines distintos a la seguridad nacional, tales como: económicos, políticos y diplomáticos.

[845] Deben definirse las penalidades de las arbitrariedades cometidas por funcionarios y particulares con respecto a las vigilancias no autorizadas o ilegitimas. Sin bien en la mayoría de legislaciones la intervención de las comunicaciones se realiza de forma excepcional y se establecen penalidades, lo cierto es que estos delitos no abarcan la intervención de otras actividades en línea, no contempladas hasta la fecha como comunicaciones y se limitan a las formas tradicionales de comunicación, tales como las escuchas telefónicas, mensajes escritos, como correos electrónicos y mensajes de texto, pero desconociendo otras formas de comunicación que por lo general son almacenadas en servidores de Internet, los que pueden ser accedidos de forma irregular por tratarse de informaciones compartidas por los usuarios con proveedores de servicios.

Si bien los principios expuestos constituyen un trabajo excepcional frente a las intervenciones de las comunicaciones, se considera oportuno que se agreguen algunos otros para complementar los aportes ya realizados.

Se estima que la **excepcionalidad** de toda forma de vigilancia debe ser otro de los principios señalados en el citado aporte, en el sentido de que cualquier medio que limite o restrinja los derechos fundamentales de las personas ha de practicarse de modo excepcional, por un tiempo prudencial y como última opción, una vez agotadas otras formas de obtener la información de una investigación. De lo contrario, la excepción podría convertirse en la regla, permitiendo de forma indefinida la intervención de las comunicaciones, como ocurrió en EE.UU. según los documentos revelados por Snowden, en los cuales se demostró que las solicitudes de intervención fueron requeridas una vez por año, de forma indefinida y regular, excediendo los límites de la razonabilidad y excepcionalidad frente a los derechos fundamentales de las personas, debilitando con ello el sistema democrático y ocasionando un grave perjuicio a las personas afectadas.

Otro de los principios que se estima necesario complemente los expuestos es el **principio de razonabilidad**, que debiera considerarse al aplicar cualquiera de los principios expuestos. Lo anterior bajo el supuesto de que toda actividad que suponga una disminución en los derechos fundamentales de las personas debe aplicarse de forma razonable, que permita o ayude a establecer un balance entre los fines perseguidos y la afectación a los derechos de las personas, para que estas medidas no resulten abusivas o arbitrarias.

Por último, se estima conveniente se adopte el **principio de mínima intervención**, de modo que se disponga en la normativa un período máximo en el cual la información requerida por parte de las autoridades debe ser destruida para garantizar, entre otras cosas, que no va a ser utilizada para fines distintos de los que permitieron su recolección, que se reduzcan las posibilidades de fugas en la información o publicaciones no autorizadas y que no colaboren a la creación de perfiles o patrones innecesarios que puedan afectar a las personas.

De otra parte, también se existen las recomendaciones realizadas por parte de organismo independientes[846], las cuales fueron requeridas por parte de la Casa Blanca luego de las revelaciones sobre la vigilancia electrónica. En vista que estas recomendaciones se dieron con propósito de la Ley de Libertad de EE.UU., fueron mencionadas en el apartado anterior. Entre los aportes más destacados se encuentran: limitar la colección de datos a granel, aumentar la transparencia, mejorar la privacidad de personas no estadounidenses, realizar una reforma organizacional y la reducción las amenazas internas.

Algunas de estas recomendaciones fueron incluidas en la reforma denominada Ley de Libertad de EE.UU., y es importante destacar que, entre ellas se señala el derecho de la privacidad de los extranjeros, dado que las autorizaciones para intervención de las comunicaciones y tráfico de Internet está desprovisto de garantías que si se respetan a los ciudadanos estadounidenses.

Otro de los aportes relevantes que es necesario señalar, es el realizado por la Oficina del Alto Comisionado de Naciones Unidas de Derechos Humanos[847], en el cual se ofrecen importantes recomendaciones sobre la aplicación del derecho internacional de los derechos humanos en relación con la privacidad de las personas. En dicho informe, se destaca:

La carencia de leyes: En este sentido se indica que no existen leyes adecuadas o, las existentes, no cuentan con las suficientes garantías procesales y

---

[846] *Vid. Supra* Cap. VI.4.1. El reporte completo de Liberty and Security in a Changing World de 12 de diciembre de 2013, puede ser consultado en: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; y el reporte completo de Privacy and Civil Liberties Oversight Board de 23 de enero de 2014 puede ser consultado en: https://www.justsecurity.org/wp-content/uploads/2014/01/Final-Report-1-23-14.pdf

[847] *Vid.* Informe de la Oficina del Alto Comisionado de Naciones Unidas de Derechos Humanos, del 30 de junio de 2014, sobre el derecho a la privacidad en la era digital, [en línea], http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

capacidades de supervisión eficaces, elementos que han contribuido a la falta de rendición de cuentas por las injerencias arbitrarias o ilegales en el derecho a la privacidad.

La existencia de lagunas en la efectividad del derecho a la privacidad: Al respecto señala dos observaciones concretas. La primera es que sigue saliendo a la luz información sobre las políticas y prácticas de vigilancia nacionales y extraterritoriales. Se están realizando investigaciones con el fin de reunir información sobre la vigilancia electrónica y la recopilación y el almacenamiento de datos personales, así como para evaluar su impacto en los derechos humanos. Distintos tribunales nacionales y regionales están examinando la legalidad de las políticas y medidas de vigilancia electrónica. En ese sentido, toda evaluación de la compatibilidad de las políticas y prácticas de vigilancia con el derecho internacional de los derechos humanos debe adaptarse necesariamente al carácter evolutivo de la cuestión. La segunda observación se refiere a la falta de transparencia gubernamental asociada a las políticas, leyes y prácticas de vigilancia, que dificulta todo intento de evaluar su compatibilidad con el derecho internacional de los derechos humanos y asegurar la rendición de cuentas.

La necesidad de un compromiso multisectorial: En este compromiso, se deberían incluir los Estados Miembros, la sociedad civil, las comunidades científica y técnica, el sector empresarial, los docentes universitarios y los expertos en derechos humanos. Será fundamental disponer de una función rectora para asegurar que dichas tecnologías se utilicen para materializar su potencial de mejora del disfrute de los derechos humanos consagrados en el marco jurídico internacional.

Toda política o práctica de vigilancia debe ser compatible con el derecho internacional de los derechos humanos: Estas prácticas deben ser compatibles con los derechos fundamentales, principalmente el derecho a la privacidad, mediante el establecimiento de salvaguardias eficaces contra los abusos. Como medida inmediata, los Estados deberían revisar sus propias leyes,

políticas y prácticas nacionales para garantizar su plena conformidad con el derecho internacional de los derechos humanos. Si detectan deficiencias, deberían tomar medidas para colmarlas, en particular adoptando un marco legislativo claro, preciso, accesible, integral y no discriminatorio. Deberían tomarse medidas para establecer regímenes y prácticas de supervisión efectiva e independiente, prestando atención al derecho de las víctimas a un recurso efectivo.

***La promoción y la protección del derecho a la privacidad en la era digital*:** Es preciso intensificar el debate y realizar un estudio a fondo sobre las cuestiones relativas a la protección efectiva de la ley, las garantías procesales, la supervisión efectiva y los recursos. Un análisis en profundidad de esas cuestiones proporcionaría una mayor orientación práctica, basada en el derecho internacional de los derechos humanos, sobre los principios de necesidad, proporcionalidad y legitimidad en relación con las prácticas de vigilancia; sobre las medidas de supervisión efectiva, independiente e imparcial; y sobre los recursos. También ayudaría a las empresas a cumplir su obligación de respetar los derechos humanos, teniendo en cuenta las salvaguardias en materia de diligencia debida y gestión de los riesgos, así como su papel en cuanto a los recursos efectivos.

Si bien los planteamientos expuestos coinciden en varios aspectos, se estima necesario resaltar que uno de los más importantes, para proteger el derecho a la intimidad y privacidad en la era digital, es la necesidad de un compromiso multilateral, en el cual se incluyan los diversos sectores de la sociedad civil, las comunidades científicas y técnicas, el sector empresarial, docentes universitarios y los expertos en derechos humanos, pues con ello se lograrán medidas oportunas y respetuosas de los derechos humanos. Los insumos que se pueden aportar frente a la seguridad nacional y la protección de los derechos humanos en general deben provenir de una sociedad participativa, de todos los sectores que la integran, fortaleciendo la democracia y participación a través de la representación, como el respeto de la dignidad humana.

De esta manera se lograrán que las posibles soluciones a los problemas de la vigilancia masiva sean aportadas desde diversas disciplinas, las que deberán indicar las formas más convenientes para que los problemas, respecto a la seguridad y la privacidad, se reduzcan y con ello evitar las supuestas fricciones que se han comentado a lo largo de esta investigación, otorgando a las personas la seguridad y privacidad propias de un Estado democrático.

De poco o nada sirve un marco jurídico de derechos humanos que sea perfecto, en el sentido de protección de derechos, si las autoridades no están dispuestas a respetarlos. De igual forma ocurre si los Estados toman medidas arbitrarias y desproporcionadas con el propósito de perseguir fines distintos a los preceptuados mediante la soberanía popular, los poderes constituidos deben en todo momento respetar el mandato popular, mandato delegado por los pueblos.

Los *sistemas de vigilancia global* no son de reciente data, por el contrario, aparecen asociados principalmente al desarrollo de las tecnologías electrónicas e informáticas. Durante la Segunda Guerra Mundial las agencias de inteligencia de los países aliados jugaron un papel importante y se estima que salvaron la vida de millones de personas, pues su intervención coadyuvó a poner fin a esa guerra dos años antes. Sin embargo, después de la segunda guerra mundial y desaparecida la guerra fría, la actividad de grupos terroristas ha propiciado que las actividades de las agencias de espionaje hayan puesto su mirada en la población civil, produciendo también un efecto colateral negativo sobre los derechos de las personas, principalmente sus derechos de privacidad. Ese arsenal de opciones para vigilar la actividad de los ciudadanos también ha sido utilizado en forma indebida, con otros fines.

Un recorrido histórico de las actividades de las agencias de inteligencia demuestra cómo se han dado abusos por parte de estos organismos, los cuales han sido aprovechados para realizar espionaje político, económico y diplomático que, lejos de los fines para los cuales fueron creados, han servido a quienes ostentan el

poder, para vigilar y controlar a los oponentes políticos, activistas de derechos humanos y periodistas.

Entre los pilares básicos de la democracia se encuentra el respeto de los derechos fundamentales y libertades individuales y entre estos, la dignidad, como derecho inviolable de la persona. Por ello, la dignidad humana se extiende más allá del cuerpo físico, representada a través de sus pensamientos y en sus entornos personales y comunicaciones, todos los seres humanos tienen el derecho a permanecer inadvertidos y a no ser molestados. De esta manera, una persona bajo vigilancia ya no es libre y una sociedad bajo vigilancia ya no es una democracia. Para mantener la validez de los derechos fundamentales, deben aplicarse todos los derechos democráticos tanto en el entorno virtual como en el espacio real.

De esta manera se estima que no corresponde hacer un equilibrio o un balance para escoger entre el derecho de intimidad y la seguridad nacional, lo que si corresponde es limitar la vigilancia masiva de conformidad con los preceptos de las libertades individuales y los principios democráticos, según las necesidades que las actividades de investigación del terrorismo, el narcotráfico, la delincuencia organizada y otras actividades ilícitas lo justifique.

Se aprecia que los marcos jurídicos generales están caracterizados por la ambigüedad o lagunas en lo que respecta a la vigilancia de las comunicaciones a gran escala, y los organismos nacionales de supervisión carecen de la capacidad para controlar, eficazmente, la legalidad de la interceptación de esos datos a gran escala por parte de los servicios de inteligencia.

Algunos activistas consideran que las facilidades que ofrecen las tecnologías de vigilancia no puede servir de base para justificar su uso. Han señalado también, que somos “sonámbulos en un estado de vigilancia”. Un número creciente de personas se niegan para aceptar la desproporcionalidad existente entre la gran colección de datos y metadatos, la duración de su retención con respecto al denominado “objetivo de prevenir el terrorismo”, que se ha convertido en la excusa

principal para la recogida de datos en masa, lo cual se ha utilizado para muchos otros propósitos distintos del objetivo principal.

Existen excepciones de los derechos de privacidad e intimidad, de los derechos de las personas para proteger sus datos personales y comunicaciones. Sin embargo, difícilmente vamos a fortalecer la “seguridad nacional” reduciendo en forma desproporcionada derechos fundamentales de las personas, porque debilitamos el estado de derecho y la democracia. El Pacto Siracusa podría servir como guía para la aplicación de límites legítimos a los derechos fundamentales, bajo el principio fundamental de que los derechos reconocidos a las personas por parte del Derecho Internacional de los Derechos Humanos no pueden ser limitados de forma arbitraria o irrazonable.

Adicionalmente, el Pacto de Siracusa señala una única posibilidad para imponer límites y excepciones a los derechos fundamentales bajo la justificación de la “seguridad nacional”. Ello se autoriza cuando se invoque este motivo para proteger la existencia de la nación, su integridad territorial o su independencia política contra la fuerza o la amenaza de la fuerza. En este Pacto se prohíbe, en forma expresa, invocar este motivo en los casos en los cuales se traten de imponer limitaciones o impedir amenazas locales o relativamente aisladas contra el orden público, así como, cuando se utiliza la seguridad nacional como pretexto para imponer limitaciones vagas o arbitrarias. De cualquier forma, según el Pacto, solo se podrá invocar cuando existan garantías adecuadas y recursos eficaces contra los abusos.

Varios organismos internacionales, organizaciones no gubernamentales, grupos de expertos y sectores de la sociedad civil han propuesto una serie de soluciones para minimizar los efectos arbitrarios y los abusos de las vigilancias masivas. Estas recomendaciones se proponen para brindar orientaciones a los Estados a fin de que las vigilancias cumplan con los derechos fundamentales de las personas. Entre los aportes más desatacados, para abordar todos los desafíos relacionados con el derecho a la privacidad, en el contexto de las tecnologías

modernas de comunicación, se plantea como necesidad la adopción de compromisos multisectoriales.

Estos compromisos deberían fortalecer el diálogo y permitir la participación todas las partes interesadas, incluidos representantes de los Estados, la sociedad civil, las comunidades científica y técnica, el sector empresarial, los docentes universitarios y los expertos en derechos humanos. A medida que evolucionan las tecnologías de las comunicaciones, será indispensable disponer de una función rectora para asegurar que estas se utilicen para la mejora del disfrute de los derechos humanos consagrados en el marco jurídico internacional.

La seguridad y la privacidad no son derechos antagónicos. En cierta medida uno depende del otro, pues si bien no son conceptos análogos y en algunos escenarios parecen ser contrarios, lo cierto es que si se ponderan estos derechos y la carga objetiva del derecho a la seguridad se impone sobre el derecho a la privacidad como derecho individual, también se disminuye la seguridad de las personas, en el sentido de exposición de sus datos y preferencias privadas, por lo cual no sería correcto decir que el derecho de privacidad debe ceder en todos los casos ante la seguridad.

La anterior afirmación se justifica en el Derecho Internacional de los Derechos Humanos, pues si bien todo individuo tiene derecho a la seguridad, también tiene derecho a no ser 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. Ahora bien, si el interés general debe privar sobre el interés individual, cómo se justificaría en los casos en los cuales el derecho de intimidad es afectado de forma masiva, pues en este caso existen dos derechos que tienen una carga de protección del mismo grado, en ambos casos existe un interés general o colectivo.

Se estima que los Estados deben fomentar las buenas conductas en Internet, pues desde el punto de vista del desarrollo y, para que la sociedad siga beneficiándose de las tecnologías, será necesario proteger a las personas frente a

diversas amenazas, buscando un equilibrio entre las intervenciones y controles informatizados y las libertades de las personas, pues de lo contrario Internet podría pasar a la historia como una invención fallida de la humanidad, restando con ello los beneficios que también ha permitido.

Estamos ante una relación similar a la que existe en el ordenamiento jurídico entre el derecho a la libertad individual por un lado y por el otro la potestad de las autoridades de detener a una persona cuando concurran ciertas circunstancias. Las personas tienen derecho de intimidad y privacidad, y las autoridades tienen la potestad de realizar vigilancias sobre las personas sólo en determinados supuestos y bajo ciertas circunstancias, pero esto solo podrá realizarse en el entendido de que cualquier exceso debe ser severamente castigado, como ocurre con los abusos de la autoridad frente a la libertad individual de las personas, donde se brinda protección desde diversos ámbitos del ordenamiento jurídico, tanto en materia civil, como en sede laboral, administrativa e incluso la penal, donde incluso se castigan como delito los actos de abuso de autoridad, la detención ilegal o arbitraria, o la simple privación de libertad, con todas sus consecuencias.

Podría concluirse que los servicios de Internet podrían transformarse y retroceder, dados los persistentes conflictos y colisiones entre los derechos de intimidad y seguridad. Drásticas decisiones podrían implementarse si aumentan los delitos, las vulnerabilidades, los peligros, frente a lo cual se estima necesario realizar todos los esfuerzos para perseguir, únicamente, a los responsables y sin afectar, de forma arbitraria, los derechos de un grupo considerable de personas.

Tal y como se ha advertido, los principios en los que se fundamenta la democracia no permiten que a las personas se les reduzcan sus derechos fundamentales por cuestiones arbitrarias, ambiguas, poco claras o que en definitiva no suponen un interés superior, pues el interés superior no está, en los casos de vigilancia masiva, a favor de la colectividad sino de quienes controlan los medios de espionaje.

Deben fomentarse las buenas conductas en Internet, tanto las realizadas por parte de los usuarios como las realizadas por parte de las empresas. Fomentar la seguridad en Internet también creará una sociedad más segura. Internet puede ser utilizado como una plataforma de lanzamiento para cambiar las conductas sociales no deseadas y mejorar la educación de las personas, promover sociedades más participativas y democráticas.

¿Sería posible entonces renunciar a los beneficios que ofrecen las tecnologías para resguardar la intimidad? La sociedad tiene la capacidad de encontrar nuevas formas de aprovechar las tecnologías, la interconectividad no es del todo indispensable, sin embargo, representa un avance considerable en cuanto a los beneficios que ha permitido, tales como la ponderación de los derechos a libertad de expresión, la participación ciudadana y el acceso a la información.

Es necesaria la participación de las empresas, la inversión en seguridad, la posibilidad de perseguir a los infractores, la necesidad de una sociedad tecnológica más segura que permite un adecuado y mejor desarrollo de las personas.

La complejidad del tema no permite brindar una única solución a la pérdida de privacidad ante la utilización indiscriminada de la vigilancia masiva, sin embargo, de resumirse en pocas palabras una única solución, podría señalarse como la necesidad de establecer ex ante en forma clara y concreta los supuestos en los cuales podría permitirse la vigilancia sobre las personas, y la posibilidad de realizar, ex post un análisis sobre la necesidad de su uso caso por caso, de manera que se establezca que estaba justificado, era proporcional e indispensable para cumplir con los fines autorizados, poniendo siempre como límite el respeto a los derechos de las personas, nacionales o extranjeros. El límite genérico de todos los derechos fundamentales es una base sólida para sostener que debe existir en los entornos virtuales un profundo respeto por los derechos de intimidad y privacidad.

Quizás el problema se deba a que quienes han utilizado estos métodos de vigilancia se hayan amparado en el combate a la criminalidad, en especial al

terrorismo, a la delincuencia organizada y al narcotráfico, entre otros, pero en un buen número tales objetivos no han constituido más que una excusa para otros propósitos no autorizados, como espiar contrarios políticos, conocer las costumbres de los consumidores, averiguar datos para extorsionar a ciertos personajes relevantes, activistas de derechos, etc.

Por esa razón no podría ser suficiente establecer autorizaciones genéricas que permitan a las autoridades realizar vigilancia masiva con la excusa de la "seguridad nacional" o para perseguir a la criminalidad organizada, el terrorismo o el narcotráfico. Deben establecerse paralelamente determinadas circunstancias que permitan, en el caso concreto, concluir de manera racional y probable que su uso estaba justificado por cuestiones fácticas comprobables, para que las autoridades puedan utilizarla.

La inversión de los Estados en cuanto a la capacidad de exploración de datos, en este momento, es mucho mayor que la inversión en tecnologías que mejoren la privacidad. En ese sentido, pareciera mucho más razonable que la inversión económica que realizan los Estados sea utilizada en la búsqueda de medidas de inteligencia que no afecten los derechos de las personas.

Se estima que los peligros de la vigilancia masiva son tan significativos como el terrorismo en sí mismo. En la actualidad no se podría saber en manos de quién están esos datos o en el futuro quien tendrá acceso a estos o que usos se les dará. Nuevas formas de terrorismo también se podrían crear a partir de la información colectada por parte del gobierno. Las revelaciones de Snowden advierten dos cosas, que toda actividad electrónica está o puede ser vigilada y que la información colectada puede ser sustraída, por lo cual tampoco existe una garantía, desde el punto de vista electrónico, de que los múltiples datos que constan en esos registros están seguros en manos del gobierno.

Debe tenerse presente que un nuevo negocio de datos se hace camino entre un mercado hasta ahora no regulado. Se ha creado una nueva forma de tráfico ilícito

de datos y las empresas ya están lucrando con esos datos, los cuales en principio son generados por la actividad legítima y descuidada de las personas, al margen de lagunas legislativas y en perjuicio de la privacidad e intimidad de las personas.

Seguirán apareciendo nuevos retos en materia de protección de la intimidad y los datos. Por ello resulta necesario que se creen nuevos mecanismos y fortalezcan los existentes para la protección de las personas y sus datos personales. Deben mejorarse las capacidades de las agencias de policía para la persecución de delitos sin lesionar los derechos fundamentales de las personas, así como la revisión permanente sobre los mecanismos y las agencias de protección.

Por último, debe recalcarse la necesidad de continuar fomentando la participación activa de los gobiernos, empresas, organizaciones, universidades, y la población civil para hacer frente a los nuevos retos en esta materia y que los aportes sean ofrecidos no solo desde diversos sectores, sino también desde diversas disciplinas, para lograr una adecuada protección de los derechos fundamentales de las personas, principalmente en relación a la privacidad y la seguridad de los entornos virtuales.

CAPÍTULO VII. CONCLUSIONES GENERALES.

"Quienes luchan para garantizar el derecho a que se respete la vida privada online están "entre la espada y la pared": por un lado se enfrentan a gobiernos restrictivos y por el otro, a empresas ávidas de beneficios."[848]

[848] Andrew Puddephatt, experto en libertad de expresión y derechos digitales.

Una primera gran conclusión se centra en la exposición que tienen las personas en la actualidad, consecuencia directa del uso de las recientes tecnologías. Si bien las personas, por un lado, se benefician cada día en mayor medida de todas las ventajas ofrecidas por las novedosas tecnologías que facilitan la vida en todo sentido, permiten el desarrollo en todos los niveles, favorecen las relaciones con los demás, en sus profesiones o actividades, con sus familias y amigos, dando a conocer y conociendo a los demás. Además de múltiples ventajas cuya lista es demasiado larga. Sin embargo, a la vez, nunca como ahora las personas se encuentran más expuestas y bastante más vulnerables, a las intromisiones indebidas a los ámbitos de intimidad y privacidad. La tecnología ha vuelto, prácticamente transparentes a los individuos.

Una segunda conclusión general es que los ámbitos de intimidad y privacidad han cambiado. Las personas ya no son tan privadas ni tan íntimas como cuando no existían las avanzadas tecnologías y las facilidades de acceder a la información, en especial la que se considera de carácter público. Conocer el estado civil del vecino nunca ha sido tan fácil como ahora, incluso saber si está casado con la persona con quien convive toma tan solo unos minutos de consulta el Registro Público correspondiente. Saber si una persona efectivamente estudió en la Universidad que dice es tan sencillo como acceder a su página y buscar la lista de graduados. Leer el periódico que está próximo a salir en edición impresa en cualquier país, es significativamente fácil. Nunca como ahora, ha sido tan fácil conocer algo sobre las personas, más si estas comparten información en las redes sociales. Ciertamente, las nuevas formas de protección de la intimidad y privacidad ahora son mucho más comunes y eficientes, permitiendo a las personas acceder a nuevas formas de protección de la información sobre sus vidas privadas, información que en la actual la sociedad electrónica tiende a disminuir, pues las personas no están conscientes de la cantidad de información que comparten todos los días sobre las actividades de su vida privada.

Desde luego que todo ello ha transformado la esfera de privacidad e intimidad, o al menos resulta bastante más difícil que las personas permanezcan desconocidas ahora que antes, y ello también significa que los ámbitos de tutela de lo que debe ser protegido y lo que no, también hayan cambiado significativamente, lo cual constituye una tercera gran conclusión. Delimitar hasta dónde debe protegerse el ámbito de privacidad y e intimidad de una persona, resulta ahora más restringido, y ello lo debe tomar muy en cuenta el ordenamiento jurídico al momento de imponer límites y sanciones.

Esta investigación ha sido centrada en un análisis sobre las implicaciones y las consecuencias jurídicas derivadas del amplio uso de los programas de vigilancia masiva, utilizados por los gobiernos, con la colaboración de las grandes empresas privadas de Internet, y ha puesto en evidencia la falta de límites precisos de esa actividad, así como la consecuente vulneración de los derechos fundamentales de las personas protegidos en la normativa de Derechos Humanos, tales como el derecho de intimidad, la protección de datos personales, la inviolabilidad de las comunicaciones, afectando con ello el desarrollo de la vida privada de las personas.

La creación de Internet ha generado un sin número de nuevas oportunidades, servicios, negocios, fuentes de información, profesiones, oportunidades, facilitando de la interconexión de las personas, se trata de un cambio que ha tenido un gran impacto político, económico y social. Con ello también se han planteado nuevos retos y también han surgido nuevas conductas delictivas y se han potenciado otras conductas negativas que existían con anterioridad.

Los gobiernos, empresas y particulares han aprovechado los recursos que ofrecen estas tecnologías para cumplir diversos objetivos. Si bien los orígenes de Internet se remontan a los años sesentas, la universalización del servicio es de los años noventa y desde entonces se han puesto de manifiesto nuevas vulnerabilidades con la utilización de las tecnologías, particularmente, en lo que respecta a los derechos de intimidad y protección de los datos personas.

Entre los problemas generados con el uso de estas tecnologías está la seguridad informática, por las inmensas posibilidades que se ofrecen en la red de redes dando pie a que aparezcan los peligros. Esto plantea serios retos a la ciencia jurídica, pues el derecho no puede constituir un obstáculo para el desarrollo de las nuevas tecnologías, ni tampoco puede convertirse en un obstáculo, que limite en forma innecesaria su verdadera dimensión, tampoco la ley debe constituir un impedimento para perseguir la criminalidad organizada, el narcotráfico, el terrorismo y muchas otras formas de delincuencia que afectan los derechos de las personas y el desarrollo de los estados. Pero por otro lado, la ciencia jurídica afronta el reto de tutelar la frágil situación en la que se encuentran los derechos de privacidad e intimidad de las personas ante el gran desarrollo de las nuevas tecnologías, y su amplia e ilimitada capacidad que tienen para atentar contra esos derechos, con el agravante de que las respuestas jurídicas han sido muy fraccionadas o regionales, limitadas por las fronteras nacionales, a diferencia del ámbito global en que se desenvuelven dichas tecnologías y las empresas que las respaldan.

La incidencia de las tecnologías en los derechos fundamentales es amplia y compleja. Las Naciones Unidas ha calificado el acceso a Internet como un derecho instrumental, como consecuencia de la libertad de expresión, lo cual indicó en un informe en mayo de 2011 de la Oficina del Alto Comisionado para los Derechos Humanos; y otra, más relevante y reciente, la Resolución del Consejo de Derechos Humanos de 5 de julio de 2012, en la cual indicó que los mismos derechos que tienen las personas offline deben también protegerse online, en particular la libertad de expresión en Internet y en otras tecnologías, así como la forma en que Internet puede ser un importante instrumento para el desarrollo y para el ejercicio de los derechos humanos.

Algunos países han incluido entre los derechos básicos de las personas el acceso a Internet, incluso algunos de estos lo han protegido constitucionalmente. Las posibilidades que ofrece Internet también ha provocado que el tema de la privacidad de la información adquiera mayor relevancia para la comunidad en

general, pues con anterioridad era un tema que se dejaba a los expertos en seguridad informática.

Asimismo, los derechos que tienen la posibilidad de ser ejercitados a través de Internet, son los más propensos a ser vulnerados. Muchos de los servicios utilizados en línea que almacenan información de los usuarios, sólo por esa razón reciben contantes ataques con el propósito de acceder a ella por ser altamente valiosa en un mercado competitivo.

A consecuencia de tanta fragilidad, se observa ahora una tendencia en las empresas, las cuales están realizando esfuerzos en proteger la información de los usuarios con el propósito de no perder clientes, quienes se sienten desconfiados ante las constantes noticias de pérdida de datos por el ataque de los hackers informáticos.

Nuevos servicios con políticas de no seguimiento y no almacenamiento de datos en la red son cada vez más frecuente y con ello consiguen nuevos clientes. Las personas son cada vez más conscientes de las afectaciones y problemas que pueden tener por la mala manipulación de sus datos personales. Es posible que noticias sobre el hackeo de diversos servicios, incluyendo los servicios ofrecidos en portales porno, han alertado a la población sobre las vulnerabilidades de los datos en Internet. De forma reciente, en el mes de mayo de 2015, un grupo de piratas informáticos llamado *The Consortium* atacó uno de los sitios web pornográficos más famoso de los EE.UU., denominado *Digital Playground,* llevándose la base de datos de 73.000 personas, que además han sido expuestas públicamente. Se indicó en las noticias que entre los datos robados se encuentran nombres de suscriptores, direcciones de correo electrónico, contraseñas, fechas de nacimiento, números de teléfono y códigos de seguridad de unas 40.000 tarjetas de crédito.

Otra de las amenazas latentes es la posibilidad que ofrecen los nuevos programas de ordenadores denominados *Big Data,* que se estiman iniciará una cuarta revolución industrial al permitir el procesamiento de cualquier base de datos

en tan solo unos instantes. Las posibilidades ofrecidas por estos programas si bien ofrecerán una ayuda importante a la humanidad, también podrían vulnerar los derechos de las personas, pues son capaces de procesas cantidades incalculables de información incluida la información sensible de las personas, de manera muy ágil y rápida.

Algunas de las recomendaciones ofrecidas para las personas que utilizan los servicios de Internet son:

- Considerar los datos que se compartirán con las empresas y la confiabilidad de estas, recordar incluso que las grandes empresas comparten datos.
- Usar seudónimos y no datos reales que permitan crear perfiles en Internet. En el caso de utilizar los seudónimos considerar la publicación de fotografías.
- Respetar la privacidad e intimidad de otras personas.
- Realizar una búsqueda de la información de las empresas con las cuales contrata los servicios a efectos de determinar las posibilidades de proteger la intimidad y qué mecanismos ofrecen en caso de vulneración, es decir examinar los términos de privacidad ofrecidos en los contratos.
- Indagar sobre las políticas de privacidad ofrecidas por las empresas con las cuales contrata servicios.
- Utilizar las opciones de configuración en modo restringido de manera que la información no sea compartida con otras personas.
- Utilizar diferentes tipos de identificación, incluyendo los usuarios y contraseñas de los servicios.
- Vigilar la actividad de los menores que navegan en Internet.
- Cambiar con frecuencia sus contraseñas y no utilizar las obvias.

El derecho a la protección de los datos personales se identifica como uno de los últimos derechos derivado del derecho de intimidad, el cual le da el soporte hasta convertirse en un derecho autónomo. De esta manera se reconoce como un derecho moderno, el cual durante su evolución atravesó distintas etapas, al principio se le consideró como un derecho para la protección de datos personales, mientras que en la actualidad se proyecta como un derecho que permite el control de los datos por parte de las personas.

El contenido de este derecho se ha ampliado con respecto a los ámbitos de cobertura, para incluir derechos como el de imagen, al estimarse que las imágenes se traducen en un conjunto de datos con los cuales una persona es identificada o identificable. El derecho a las comunicaciones de forma reciente empieza a ser protegido por los mecanismos que tutelan los datos personales al aceptar que los datos de las comunicaciones (metadatos) no incluyen el contenido de las conversaciones.

El desarrollo de los servicios de Internet y de las comunicaciones han generado el crecimiento de datos mediante los cuales se pueden construir perfiles de las personas a partir de información que, en la mayoría de los casos no eran conscientes que estaba siendo compartida.

La actividad de las empresas en Internet es fundamentalmente la auto-regulada y si bien ha sido una técnica de relativa efectividad, lo cierto es que tiene también algunos desatinos. La imposición de límites a las actividades de las empresas en Internet, representa un desafío a los juristas y gobiernos, puesto que los problemas de jurisdicción y aplicación de los preceptos jurídicos han de ser tamizados para posibles aplicaciones, esencialmente, cuando se trata de determinar la responsabilidad extracontractual.

El valor de mercado de los datos de las personas ha intensificado los ataques en contra de las bases de datos informatizadas, a lo cual se suma la importancia en la obtención y manejo de ciertos datos para el desarrollo, principalmente, de las

actividades económicas, incluidas las de los gobiernos. Solo en EE.UU. existen más de 8000 empresas dedicadas a la correduría de datos, son los llamados *data brokers*, las que analizan los datos y luego los venden, tomando como base información que en principio fue facilitada por las personas, pero luego de ser procesada permite crear perfiles con alto valor económico para las empresas.

Al respecto se han planteado posibles soluciones para disminuir la afectación de los derechos de las personas. Entre estas se encuentra: reformas jurídicas, establecer controles, imponer límites y delimitar nuevas jurisdicciones. Soluciones que deben además implementarse con la participación de los diversos sectores involucrados.

Los mecanismos jurídicos son reactivos y no preventivos lo cual representa una desventaja en la protección de los datos de las personas. Para lograr una mejora significativa en relación a la utilización de las tecnologías, resulta necesario que las empresas relacionadas a los servicios de TIC colaboren con la protección de datos personales y diseñen servicios y aparatos que cuenten con mecanismos de protección a la privacidad por defecto y desde el diseño. Debe advertirse que la mayoría de controles legales para la protección de los datos personales actúan luego de que se han producido las vulneraciones, razón por la cual también es necesario que esta protección se realice en el origen y por defecto.

Los derechos fundamentales como todos los derechos pueden ser limitados, sin embargo, estas limitaciones deben ser legítimas, necesarias, razonables y proporcionadas, de manera que estén dispuestas por ley, sean claras y limitadas. Toda excepción debe estar fundamentada en una resolución para que los afectados tengan oportunidad de oponerse o ser indemnizados en los casos en los cuales no se justificaba la medida.

El consentimiento informado actúa como excepción respecto al derecho de protección de datos personales, razón por la cual cualquier vicio no advertido en el consentimiento se traduce una “autorización” para la disposición de esos datos. La

mayoría de las empresas busca obtener ganancias con los datos de las personas, pues el costo de la información es importante, así como los beneficios propios de las empresas al contar con esa información para el análisis de sus operaciones.

Debe advertirse que los derechos que protegen la intimidad se enfrentarán a nuevas posibilidades de las tecnologías, como por ejemplo la posibilidad de los aparatos de almacenar los pensamientos de las personas. Un nuevo tipo de protección deberá ser desarrollada frente a la posibilidad de que se puedan captar y almacenar los pensamientos y los recuerdos de las personas. Nuevos servicios se ofrecerán próximamente, pues ya han sido anunciados por algunas empresas que indican tener en corto plazo tecnologías capaces de conectarse a través de una interface con los cerebros de las personas. Es probable que no exista otra forma más directa de exponer a la intimidad de una persona que accediendo a sus recuerdos y pensamientos.

No debe olvidarse que el caso del derecho al olvido en Internet resuelto por el TJUE constituye uno de los primeros antecedentes jurídicos contra una de las grandes empresas de Internet, en el cual se delimitó la competencia de la normativa comunitaria, obligándose la empresa Google a remover las referencias del pasado del afectado, sin embargo, el medio La Vanguardia no fue obligado a remover la referencia en la cual publicó el anuncio que reclamaba el afectado.

Pese a que en el caso de Google se produjo un efecto multiplicador con respecto a la publicación que se quería en un inicio borrar de Internet, se estima que los esfuerzos continuos en esta materia disminuirán el efecto Streinsad, para realizar una protección de la intimidad de las personas.

Como se ha indicado, el uso de las tecnologías también ha sido aprovechado por parte de los gobiernos con el propósito de cumplir sus objetivos. De esta manera se ha implementado la utilización de programas de vigilancia masiva por parte de las agencias de inteligencia. Esta situación fue denunciada por parte del ex analista de la NSA Edward Snowden, quien reveló documentos secretos de los EE.UU. en

los cuales se evidenciaba la recopilación a granel de los datos de las personas. En esta primera revelación filtró documentos en de los cuales se indica que las escuchas y recolecciones estaban dirigidas contra mandatarios de otros países, como Brasil, México y Alemania.

Si bien los sistemas de vigilancia global no son de reciente data, lo cierto es que con anterioridad no se contaba con tecnologías que permitieran tal grado de control. Un repaso histórico de las actividades desplegadas por parte de las agencias de inteligencia, permite observar abusos, aprovechados por quienes ostentan el control de las agencias de espionaje.

Los Estados basados en una democracia constitucional, no pueden pretender controlar a la población a través de vigilancias que atenten contra sus derechos fundamentales, pues este control por lo general se traduce en una afectación económica y social, todo ello contra los principios que inspiran las democracias modernas. Se estima que una persona bajo vigilancia ya no es libre y una sociedad bajo vigilancia ya no es una democracia. Para mantener la validez de los derechos fundamentales, deben aplicarse todos los derechos democráticos en el entorno virtual como en el espacio real.

Cualquier tipo de excepción que permite la disminución de garantías fundamentales en un Estado debe ser informada y acordada de conformidad con las reglas y lineamientos generales que sirven de guía en los casos en los cuales no existe otra posibilidad que ejecutar medidas que afecten derechos fundamentales. En ese sentido, el Pacto Siracusa podría funcionar como guía para la aplicación de límites al ejercicio de los derechos fundamentales, lo anterior siempre bajo el principio fundamental de que los Derechos Humanos no pueden ser limitados de forma arbitraria o irrazonable.

Es indudable que los intereses particulares ceden ante los intereses colectivos, sin embargo, en los casos de vigilancia electrónica masiva los derechos afectados son los de una colectividad. Si la seguridad de un Estado se encuentra

en peligro y corre un riesgo inminente la nación, la integridad territorial o la independencia política, sería justificable la utilización de medidas que puedan desplazar o minimizar los derechos de las personas. Ahora bien, en el momento en que esas medidas no sean necesarias, deberán restituirse los derechos que fueron suspendidos, regresando la situación a su protección original.

Algunos organismos internacionales, organizaciones no gubernamentales, grupos de expertos y sectores de la sociedad civil han propuesto una serie de soluciones para minimizar los efectos arbitrarios de las vigilancias masivas. Se destacan los aportes más relevantes a efectos de abordar todos los desafíos relacionados con el derecho de privacidad e intimidad. Entre los principales se destaca la necesidad de adoptar compromisos multisectoriales, en los cuales se incluyan no solo a diversos sectores de la comunidad sino también los grupos de expertos en diversas áreas para que se presenten soluciones complementarias con el fin de disminuir los efectos negativos que tienen los programas utilizados por parte de las agencias de inteligencia.

Si bien se reconoce que todo individuo tiene derecho a la seguridad, también tiene derecho a no ser 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, de manera que sólo ante casos excepcionales, debidamente previstos en la ley, podrían admitirse limitaciones. Estos derechos son reconocidos por tener una carga de protección del mismo grado, pues en ambos casos existe un interés general o colectivo, si se atiende a que la afectación al derecho de intimidad repercute de forma negativa en millones de personas, incluyendo tanto a nacionales como a extranjeros.

Los esfuerzos económicos para poder realizar la vigilancia masiva son, por mucho, mayores a la inversión que se realiza en la protección de la intimidad de las personas. Pareciera entonces razonable que la inversión económica que realizan los Estados sea utilizada en la búsqueda de medidas de inteligencia que no afecten

los derechos de las personas, al menos cuando ello no sea necesario y proporcional.

Se estima que el principal peligro de la vigilancia electrónica es el debilitamiento de los sistemas constitucionales democráticos pues, aunque esta vigilancia se realice con la indulgencia de un sector de la población, no sería compatible con los pilares esenciales de la democracia, afectando con ello la institucionalidad y excediendo las potestades de imperio propias de un Estado de derecho. Un sistema de vigilancia como el descubierto por Snowden solo es imaginable en el distópico mundo de Orwell, en el panóptico de Bentham, o en las novelas de ciencia ficción.

Las revelaciones sobre la existencia de la vigilancia masiva deben ensanchar el panorama y atraer la atención de las personas a dos cosas: la primera, que toda actividad electrónica está o puede ser vigilada y; la segunda, que toda la información colectada puede ser ilegalmente sustraída. La desproporcionalidad y la necesaria recogida de datos más grande de la historia de la humanidad denunciada por Snowden, definitivamente, tendrá efectos que repercutirán a través de los años, siendo casi imposible lograr una reparación de los derechos que han sido vulnerados.

Sin duda alguna, seguirán apareciendo nuevos retos que podrán a prueba los mecanismos de protección de la intimidad y los datos. Por lo anterior, resulta necesario que se fortalezcan los mecanismos existentes y se creen nuevas formas de protección de los datos de las personas, así como se instauren programas permanentes para la revisión de los mecanismos y las agencias de protección.

Desde luego es prácticamente inviable una postura rígida que impida la vigilancia masiva y el análisis de datos existentes en Internet.

Existen supuestos que justifican que esa actividad se realice, como resulta ser el combate a la delincuencia organizada, al narcotráfico, al terrorismo, al fraude fiscal, en fin, la criminalidad en general. También es posible que las empresas y los

particulares puedan obtener y utilizar la información general de las personas, cuando no se afecten sus derechos individuales de privacidad e intimidad, aunque lo hagan con fines comerciales o económicos en general.

El verdadero desafío de los Estados y del ordenamiento jurídico se encuentra en que la solución nunca podrá ser unilateral o de un país en particular, dada las formas en que se realizan esas actividades que se quieren regular. La actividad de vigilancia masiva y análisis de datos es una actividad global, y global debe ser la posible regulación del fenómeno.

Por ello se estima importante que exista una adecuada regulación global que establezca limitaciones tanto *ex ante* como *ex post*.

Es indispensable en primer término distinguir entre los sujetos involucrados en la realización de la vigilancia masiva y el análisis de datos.

Estos sujetos pueden ser:

a. El Estado, por razones de interés público, seguridad nacional, fiscales u otras razones propias del Estado.

b. Las empresas de internet, con fines propios y para beneficio de otros y;

c. Los particulares, con interés comercial, o por otras razones, incluso personales o procesales.

Los controles *ex ante* no pueden ser iguales para cada uno de los sujetos señalados.

Dichos controles deben ser, en primer lugar, normas legales claras, dirigidas a cada grupo de sujetos, mediante las cuales se les indique en qué supuestos, cuándo y con cuáles limitaciones pueden realizar vigilancia, almacenar datos, analizarlos y entregarlos a otros.

La simple existencia de la normativa debiera constituir un mecanismo de autorregulación, mediante el cual los propios sujetos restrinjan su actividad de almacenamiento y análisis de datos, conforme se disponga en la ley.

En segundo lugar, podrían preverse controles *ex ante* realizables por ciertos órganos, administrativos y jurisdiccionales, los cuales podrían autorizar a los sujetos (Estado, grandes empresas de Internet y a los particulares) a realizar el almacenamiento de los datos, imponerse de su contenido, analizarlos y entregarlos a otros, por razones particulares o comerciales, o para ser utilizados en un procedimiento administrativo o judicial.

Los controles *ex post* pueden ser administrativos, aplicables en primera instancia por órganos dedicados a supervisar la actividad en Internet y a la protección de datos, y en última instancia pueden ser aplicados por órganos jurisdiccionales. Su labor debe dirigirse a verificar en cada caso el que la actividad se haya ajustado a los supuestos previstos en la ley, y que en el caso concreto resultaba necesaria, proporcional y razonable, de todas maneras, siempre dentro de los términos de un Estado de derecho.

BIBLIOGRAFÍA.

1. LIBROS Y ARTÍCULOS.

ABAD YUPANQUI, Samuel B., "El derecho al secreto de las comunicaciones. Alcances, límites y desarrollo jurisprudencial" en *Pensamiento Constitucional* - No. 16, enero, 2012.

ABRIL, Patricia S., y PIZARRO MORENO, Eugenio, "La intimidad europea frente a la privacidad americana. Una visión comparativa del derecho al olvido*"* en *InDret Revista para el análisis del derecho*, Barcelona, enero 2014, [en línea], http://derechoaleer.org/media/files/olvido/1031.pdf

AGUSTINA SANLLEHÍ, José Ramón, *Privacidad del trabajador vs. deberes de prevención del delito en la empresa,* Editorial B de F, Buenos Aires, 2009.

ALBORNOZ, María Belén, "Cibercultura y las nuevas nociones de privacidad" *Universidad Central Colombia,* número 28, abril, 2008, [en línea], http://www.ucentral.edu.co/images/editorial/nomadas/docs/nomadas_4_ciber_belen.pdf

ALLEN, ANITA L., *Unpopular Privacy: What must we hide?,* Oxfort University Press, New York, 2011, [versión para lector digital Kindle].

ALTMAN, Irwin y TAYLOR, Dalmas A., *Social penetration: The development of interpersonal relationships,* Holt, Rinehart and Winston, Nueva York, 1973.

ALTOAGUIRRE, Marta, *Periodismo, Derechos Humanos y control del poder político en Centro América,* Inter-American Institute of Human Rights, Texas, 1994.

ÁLVAREZ GONZÁLEZ, Clara Luz, *Internet y derechos fundamentales*, Porrúa, México D.F., 2011.

ÁLVAREZ RODRÍGUEZ, Lilibeth, "Derecho al Olvido como garantía para la Autodeterminación Informativa en las Redes Sociales" en *IV Foro Internacional de derechos humanos y tecnologías de la información y la comunicación, México,* [en línea], http://www.repositoriodigital.ipn.mx/bitstream/handle/123456789/3987/Memoria%204to%20Foro%20DHTIC%2015.pdf?sequence=1

ÁLVAREZ-SALA WALTHER, Juan, *et ál.*, *Derecho de la empresa y protección de datos,* Editorial Thomson, España, 2008.

ARAUJO CARRANZA, Ernesto, "El derecho a la información de la protección de datos personales en el contexto general y su construcción teórica y jurídica" en *Revista Ius, Instituto de Ciencias Jurídicas de Puebla A.C* - No. 23, enero, 2009.

ARDÓN ACUÑA, Luis, "La Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales. ¿Brinda una protección real y efectiva para el derecho a la autodeterminación informativa en Costa Rica?", *Tesis Maestría,* Universidad Nacional de Lomas de Zamora, 2013.

ARELLANO TOLEDO, Wilma y OCHOA VILLICAÑA, Ana María, "Derechos de privacidad e información en la sociedad de la información y en el entorno TIC", IUS, *Revista del Instituto de Ciencias Jurídicas de Puebla*, No. 31, enero – junio, 2013.

ARELLANO TOLEDO, Wilma, "Computación en la nube, derecho y privacidad: especial referencia a México y Europa*",* en AMOROSO FERNÁNDEZ, Yarina (coord), *Género, código y juventud. Construir sociedades más justas e inclusivas,* Unión de Juristas de Cuba (UNIJURIS) y Sociedad Cubana de Derecho e Informática, La Habana, 2014.

ARMAGNAGUE, Juan Fernando (dir.), *Derecho a la Información, Hábeas Data e Internet,* Ed. la Rocca, Buenos Aires, 2002.

AUSLOOS, Jef, "The right to be forgotten – Worth Remembering?", *Computer Law & Security Review*, vol. 28, No. 2, 2012, [en línea], http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1970392

AVELEYRA, Antonio M., "El derecho de acceso a la información pública vs. El derecho de libertad informática", *Revista de la Universidad Iberoamericana,* México, 2003, [en línea], http://www.juridicas.unam.mx/publica/librev/rev/jurid/cont/32/pr/pr24.pdf

BADENI, Gregori, *Nuevos Derechos y Garantías Constitucionales*, Editorial AD-HOC S.R.L., Buenos Aires, 1995.

BARRANCO FRAGOSOM, Ricardo, *¿Qué es Big Data?*, México, 2012, [en línea], http://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/index.html

BARRIUSO RUÍZ, Carlos, "Las Redes Sociales y la Protección de Datos Hoy" en *Anuario de la Facultad de Derecho, Universidad de Alcalá II*, 2009, [en línea], http://biblio.juridicas.unam.mx/libros/6/2940/7.pdf

BARRIUSO RUÍZ, Carlos, *Interacción del derecho y la informática*, Dykinson, Madrid, 1996.

BASTERRA, Marcela I., *Protección de Datos Personales,* Editorial Ediar, Buenos Aires, 2008.

BAZÁN, José Luis, "Correo electrónico y política de privacidad en las empresas" en *Revista de Derecho* [documento electrónico de Vlex].

BAZÁN, Víctor, "El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado" en *Estudios Constitucionales,* Año 3 No.

2, Universidad de Talca, 2005, [en línea], http://www.cecoch.cl/docs/pdf/revista_ano3_2/revista_ano3_2_4.pdf

BEJAR, Helena, “Individualismo, privacidad e intimidad: precisiones y andaduras” en CASTILLA DEL PINO, Carlos, *De la intimidad*, Crítica, Barcelona, 1989.

BELDA PÉREZ-PEDRERO, Enrique, “El derecho al secreto de las comunicaciones”, en *Parlamento y Constitución,* No. 2, 1998, [en línea], http://dialnet.unirioja.es/servlet/articulo?codigo=197133

BELL, Daniel, *El advenimiento de la sociedad post-industrial: un intento de prognosis social,* Alianza, Madrid, 1976.

BERTI, Federico, “Comisión Interamericana de DDHH cuestionó actividad de espionaje de EEUU” en *Revista Científica Equipo Federal del Trabajo* - No. 107, Abril 2014.

BIBBY, Andrew, “Correo electrónico e Internet en el trabajo: ¿privado o público serrar signo de pregunta?”, en *Revista de la OIT,* No. 40, Agosto 2001.

BLANCO LOZANO, Carlos, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, Tratado de Derecho Penal Español,* Tomo 2 – vol. 1, 2005.

BOZA, Beatriz, Acceso a la Información del Estado. Marco legal y buenas prácticas, Konrad-Adenauer, Lima, 2004, [en línea], http://www.kas.de/wf/doc/kas_5698-1522-4-30.pdf?050317214915

BREWER CARÍAS, Allan, *Mecanismos nacionales de protección de los derechos humanos,* Instituto Interamericano de Derechos Humanos, San José, 2005.

BRUNNER, José Joaquín, *Cibercultura: la aldea global dividida*, Mesa redonda sobre Cibercultura, Hannover, 2000, [en línea],

http://mt.educarchile.cl/archives/CIBERCULTURA%20O%20UNA%20ALDEA%20GLOBAL%20DIVIDIDA.pdf

BUSTAMANTE DONAS, Javier, “Derechos Humanos en el ciberespacio”, en GRACIANO GONZÁLEZ, *La condición humana en la sociedad tecnológica*, Madrid, Tecnos, 1999.

BUSTAMANTE DONAS, Javier, “Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica”, en *Revista Iberoamericana de Ciencia, tecnología, Sociedad e Innovación*, No. 1, Septiembre-Diciembre 2001, [en línea], http://www.campus-ei.org/revistactsi/numero1/bustamante.htm

CAFFERATA NORES, José I., *Proceso Penal y Derechos Humanos,* Editores del Puerto s.r.l., Buenos Aires, 2000.

CALANDRINO, Joseph, *et ál.,* “*You might also like: Privacy risks of collaborative filtering”* Security and Privacy, IEEE Symposium, 2011, [en línea], https://www.cs.utexas.edu/~shmat/shmat_oak11ymal.pdf

CAMPUZANO TOMÉ, Herminia, *Vida privada y datos personales*, ed. Tecnos, Madrid, 2000.

CANTÚ AGUILLÉN, Ricardo, *Derecho de la información en América Latina y en México,* Universidad Autónoma de Nuevo León, México, 2006.

CARBALLO, Elvira, "Informática y Protección de datos: Antecedentes para el proyecto de una ley nacional", *Revista del Colegio de Abogados de Buenos Aires*, núm. 3, 1986.

CARBONELL SÁNCHEZ, Miguel, *Los derechos fundamentales en México,* UNAM-Porrúa-CNDH, 2005.

CARRASCO GALLARDO, Milushka, *El proceso de hábeas data,* Gaceta Notarial, Lima, 2012.

CARRERAS SERRA, Lluís, *Intromisiones legítimas en los derechos de la personalidad,* Derecho español de la información, 2003.

CARVAJAL PÉREZ, Marvin, "Tutela Constitucional del Derecho a la Autodeterminación Informativa en Costa Rica", en *Temas de Derecho Constitucional Costarricense*, Asociación de Letrados de la Sala Constitucional Tomo I, San José, 2007.

CARVAJAL PÉREZ, Marvin, *Tutela constitucional del derecho a la autodeterminación informativa en Costa Rica,* 2008*,* [en línea], http://www.derecho-comparado.org/Colaboraciones/carvajalPÉREZPonChile.htm

CASTAN TOBEÑAS, José, "Los derechos de la personalidad", *Revista General de Legislación y Jurisprudencia,* núm. 1-2, 1952.

CASTELLS, Manuel, "Internet y la Sociedad-Red", en *Revista La Factoría*, No. 14-15, febrero-setiembre, 2001, [en línea], http://www.revistalafactoria.eu/articulo.php?id=185

CASTELLS, Manuel, La Galaxia Internet Reflexiones Sobre Internet, Empresa y Sociedad, Editorial Areté, Barcelona, 2001.

CASTILLO JIMENES, Cintia, "Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información", *En Derecho y Conocimiento*, vol. 1, Facultad de Derecho de la Universidad de Huelva, 2001, [en línea], http://www.uhu.es/derechoyconocimiento/DyC01/A02.pdf

CASTRO BONILLA, Alejandra, "El uso legítimo del correo electrónico", Ponencia del II Congreso Mundial de Derecho Informático [en línea], www.ieid.org/congreso/ponencias/Castro%20Bonilla,%20Alejandra.pdf .

CASTRO BONILLA, Alejandra, “Los Derechos Fundamentales en Internet. Costa Rica”, *Revista Electrónica de Derecho Informático,* No. 50, [en línea], http://www.hacienda.go.cr/centro/datos/Articulo/Los%20Derechos%20Fundamentales%20en%20Internet.doc

CAVOUKIAN, Ann, “Privacy by Design”, en *Information and Privacy Commissioner of Ontario,* 2011, [en línea], https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf

CELIS QUINTAL, Marcos Alejandro, “La protección de la intimidad como derecho fundamental de los mexicanos” [en línea], http://biblio.juridicas.unam.mx/libros/5/2253/9.pdf

CHINCHILLA SANDÍ, Carlos, “Personalidad Virtual: Necesidad de una reforma constitucional” en *Revista de Derecho y Tecnologías de la Información,* N° 3-2005. UNED, San José, 2005, [en línea], http://www.egov.ufsc.br/portal/conteudo/personalidad-virtual-necesidad-de-una-reforma-constitucional

CHINCHILLA SANDÍ, Carlos, *Delitos informáticos: elementos básicos para identificarlos y su aplicación en Costa Rica*, Farben Grupo Editorial Norma, San José, 2004.

CHIRINO SÁNCHEZ, Alfredo, “La Ley de Protección de Datos de Costa Rica. Luces en las sombras” en *Revista Internacional de Protección de Datos Personales,* Universidad de los Andes. Facultad de Derecho, No. 1 julio - diciembre de 2012.

CHIRINO SÁNCHEZ, Alfredo, *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica,* Comisión Nacional para el Mejoramiento de la Administración de Justicia, San José, 1997.

CHIRINO SÁNCHEZ, Alfredo, *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica.* Límites al Derecho a la Intimidad de los Trabajadores. Escuela Judicial del Poder Judicial, San José, 1980.

CHIRINO SÁNCHEZ, Alfredo, *La protección de datos al amparo de la Constitución Política, en Constitución y Justicia Constitucional*, Colegio de Abogados de Costa Rica, San José, 2009.

CIFUENTES, Santos, *Derechos Personalísimos*, ed. Astrea, Buenos Aires, 1995.

CIFUENTES, Santos, *El derecho a la vida privada, tutela a la intimidad,* ed. La Ley, Buenos Aires, 2007.

COOLEY, Thomas M., *The elements of torts,* Callaghan and Company, 1895.

CÓRDOBA ORTEGA, Jorge y GONZÁLEZ PORRAS, Andrés, *Constitución Política de la República de Costa Rica. Concordada y con Jurisprudencia de la Sala Constitucional,* Investigaciones Jurídicas S.A., San José, 2010.

CÓRDOBA ORTEGA, Jorge y GONZÁLEZ PORRAS, Andrés, *Ley de la Jurisdicción Constitucional. Con jurisprudencia, concordada y Actas de discusión legislativa,* Investigaciones Jurídicas S. A., 2008.

CÓRDOBA ORTEGA, Jorge, “El Derecho Público a Comienzos del Siglo XXI”, en *Apuntes sobre el Recurso de Hábeas Data en el Derecho Costarricense y en el Derecho Comparado,* Civitas Ediciones S.L. Madrid, 2003.

CÓRDOBA ORTEGA, Jorge, *Código de derecho público,* Investigaciones Jurídicas S.A., San José, 2013.

CÓRDOBA ORTEGA, Jorge, CÓRDOBA UMANZOR, Jorge y GONZÁLEZ PORRAS, Andrés, *Constitución Política de la República de Costa Rica. Incluye Descriptores, glosario y guía de redacción de recursos de amparo,* Educatex, San José, 2011.

CÓRDOBA ORTEGA, Jorge, *El Derecho de acceso a la Información Pública en el ordenamiento jurídico costarricense. Situación actual, desarrollo y tendencias,* Instituto de Prensa y Libertad de Expresión (IPLEX), San José, 2008.

CÓRDOBA ORTEGA, Jorge, *La Legislación Costarricense y el Derecho de Acceso a la Información Pública,* Instituto de Investigaciones Jurídicas, San José 2004.

CORREA, Carlos María, *Derecho Informático,* Buenos Aires, 2ª ed., 1987.

COTINO HUESO, Lorenzo, "*Libertad en Internet*", Edit. Tirant lo Blanch, Madrid, 2007.

DARANAS PELÁEZ, Manuel (trad.), "Jurisprudencia constitucional extranjera. Tribunal Constitucional Alemán", Ley del Censo, BJC, número 33, 1984.

DAVARA RODRÍGUEZ, Miguel Ángel, "El tratamiento de datos de carácter personal y la utilización de la tecnología: entre la ética y el derecho" en *Diario La Ley*, Nº 8157, 26 de Setiembre, 2013, [en línea], http://www.juntadeandalucia.es/institutodeadministracionpublica/aplicaciones/boletin/publico/boletin56/Articulos_56/Davara-Rodr%C3%ADguez.pdf

DAVARA RODRÍGUEZ, Miguel Ángel, *Manual de Derecho Informático,* Editorial Aranzadi, Madrid, 10ª ed., 2008.

DE ANDRÉS BLASCO, Javier, "¿Qué es Internet?", en GARCÍA MEXÍA, Pablo (dir.), *Principios de Derecho de Internet,* Segunda Edición, Tirant lo Blanch, Valencia, 2ª ed., 2005.

DE ESTEBAN Jorge y GONZÁLEZ-TREVIJANO, Pedro J., *Curso de Derecho Constitucional Español III,* Editorial AGISA, Universidad Complutense de Madrid, 1994.

DE MIGUEL ASENSIO, Pedro, *Derecho privado de Internet,* Civitas, Madrid. 2001.

DÍAZ REVORIO, Francisco Javier, "¿Puede ser inconstitucional la Constitución?". *Justicia constitucional, Revista de jurisprudencia y doctrina,* No. 1, año uno, septiembre, Lima, 2005.

DÍAZ REVORIO, Francisco Javier, "El Derecho Fundamental al Secreto de las Comunicaciones: Una Visión Desde la Jurisprudencia Europea y su Influencia en el Tribunal Constitucional Español", en *Revista del Centro Nacional de Derechos Humanos,* [en línea], http://www.juridicas.unam.mx/publica/librev/rev/derhumex/cont/2/art/art5.pdf

DÍAZ REVORIO, Francisco Javier, "El derecho fundamental al secreto de las comunicaciones", En *Derecho PUC,* Revista de la Facultad de Derecho, No. 59, 2007.

DÍAZ REVORIO, Francisco Javier, "Sobre el concepto de deber constitucional y los deberes en la Constitución de 1978", *Pensamiento Constitucional* - No. 16, enero, 2012.

DÍAZ REVORIO, Francisco Javier, "Tecnologías de la información y la comunicación y nuevas dimensiones de los derechos fundamentales". *Ponencia presentada al X Congreso Iberoamericano de Derecho Constitucional, en la Mesa 6: Derechos fundamentales,* llevado a cabo en Lima, del 16 al 19 de septiembre de 2009.

DÍAZ REVORIO, Francisco Javier, *Los derechos humanos ante los nuevos avances científicos y tecnológicos. Genética e internet ante la constitución,* Tirant Lo Blanch, Valencia, 2009.

DÍAZ ROJO, José Antonio, *Privacidad: ¿neologismo o barbarismo?, Consejo Superior de Investigaciones Científicas*, 2002, [en línea], https://pendientedemigracion.ucm.es/info/especulo/numero21/privaci.html

DÍEZ-PICAZO GIMÉNEZ, Luis María, *Sistema de derechos fundamentales,* 2ª edición, Civitas, Madrid, 2005.

DRUMMOND, Víctor, *Internet, privacidad y datos personales,* Editorial Reus, S. A. Madrid, 2004.

ECHAVERRÍA, Javier, "Educación y tecnologías telemáticas", *Revista Iberoamericana de Educación,* septiembre- diciembre, No. 24, 2000.

ECHEVERRÍA, Javier, *Los señores del aire: Telépolis y el tercer entorno,* Editorial Destino, Barcelona, 1999.

EKMEKDJIAN, Miguel Ángel y PIZZOLO, Calogeno, *Hábeas Data. El derecho a la intimidad frente a la revolución informática*, Ediciones Depalma, Buenos Aires, 1996.

ENGELS, Federico, *Anti-Dühring,* Ediciones Pueblos Unidos, Montevideo, 1948.

ESPIN TEMPLADO, Eduardo, *Lecciones de Derecho Político,* Tirant lo Blanch, Valencia, 1994.

ESTUDILLO GARCÍA, Joel, "Surgimiento de la sociedad de la información", Biblioteca Universidad, *Nueva Época*, vol. 4, No. 2, julio-diciembre 2001.

FAYOS CARDO, Antonio, *Derecho a la intimidad y medios de comunicación,* Centro de Estudios Políticos y Constitucionales, Madrid, 2000.

FELDSTEIN DE CÁRDENAS, Sara L. y SCOTTI, Luciana B., *Internet, comercio electrónico y derecho la intimidad: un avance de los tribunales argentinos,* [Biblioteca Vlex].

FELDSTEIN DE CÁRDENAS, Sara L., *Internet: un Golem de la postmodernidad,* [Biblioteca Vlex].

FERNÁNDEZ ACEBO, María Dolores, “La tutela de los derechos fundamentales a la intimidad e integridad física frente a la actuación de los poderes públicos sobre el cuerpo humano. Una perspectiva constitucional sobre las intervenciones corporales y otras diligencias de investigación”, *Tesis Doctoral,* Universidad de A Coruña, 2013.

FERNÁNDEZ BRENES, Silvia, LEIVA MÉNDEZ, Silvia, et. ál., “La tutela administrativa de la autodeterminación informativa”, *Democracia Digital* [Biblioteca Vlex]

FERNÁNDEZ ESTEBAN, María Luisa, “Internet y los derechos fundamentales”. *Anuario Jurídico de La Rioja*, No. 6-7, 2000-2001, pp. 321-356.

FERNÁNDEZ ESTEBAN, María Luisa, “La regulación de la libertad de expresión en Internet, en Estados Unidos y en la Unión Europea”, *Revista estudios políticos*, No. 103, 1999.

FERNÁNDEZ ESTEBAN, María Luisa, *Nuevas tecnologías, Internet y derechos fundamentales,* Mc Graw Hill, Madrid, 1998.

FERRAJOLI, Luigi, “Sobre los derechos fundamentales”, *Revista Cuestiones Constitucionales,* Universidad Nacional Autónoma de México, julio-diciembre, No. 015. pp. 113-136.

FERRERIA RUBIO, Delia Matilde, *El derecho a la intimidad,* Editorial Universidad, Buenos Aires, 1982.

FIX FIERRO, Héctor, “El juicio de amparo mexicano y el recurso constitucional federal alemán”, *Boletín Mexicano de Derecho Comparado*, Instituto de Investigaciones Jurídicas UNAM, No. 77, 1993, [en línea], http://biblio.juridicas.unam.mx/revista/DerechoComparado/numero/77/art/art3.htm

FLORES DAPKEVICIUS, Rubén, *Amparo, hábeas corpus y hábeas data,* Editorial B de F Ltda., Montevideo - Buenos Aires, 3ª edición, 2011.

FOUCAULT, Michael, "Nuevo orden interior y control social" en *El viejo topo*, No. 7; también en *Vigilar y castigar,* París. 1era edición - en francés -, 1975.

FREIXAS GUTIÉRREZ, Gabriel, La Protección de Datos de Carácter Personal en el Derecho Español, Editorial Bosch, Barcelona, 2001.

FRIED, Charles, "Privacy", en *Yale Law Journal*, vol. 77, 1967-1968.

FRONSINI, Vittorio, "Bancos de Datos y Tutela de la Persona", *Cuadernos y Debates del Centro de Estudios Constitucionales de Madrid,* [en línea], http://www.cepc.es/rap/Publicaciones/Revistas/3/REPNE_030_022.pdf

GALÁN JUÁREZ, Mercedes, *Intimidad: Nuevas dimensiones de un viejo derecho",* Universitaria Ramón Areces, Madrid, 2005.

GALINDO DÍAZ, Liliana, et. ál., "Los derechos de autor en el entorno digital y el Internet en Colombia: una mirada al estado del arte actual y sus principales problemas", *Revista de Derecho, Comunicaciones y Nuevas Tecnologías* - No. 10, diciembre 2013.

GARCÍA BARRERA, Myrna Elia, *Derecho de las nuevas tecnologías,* Instituto de Investigaciones Jurídicas, Universidad Autónoma de México, México, 2008.

GARCÍA MEXÍA, Pablo (dir.), *Principios de Derecho de Internet,* Tirant lo Blanch, Valencia, 2ª ed., 2005.

GARCÍA MEXIA, Pablo y CORONA HERRERO, Ulises, "Internet y el derecho de las telecomunicaciones: El régimen jurídico del acceso a la Red" en GARCÍA MEXÍA, Pablo (dir.), *Principios de Derecho de Internet*, Tirant lo Blanch, Valencia, 2a ed., 2005.

GARCÍA MEXÍA, Pablo, “Internet y protección de datos. Los desafíos de la evolución digital”, *Diario La Ley*, año XXXII, No. 7577, 25 de febrero de 2011.

GARCÍA MEXÍA, Pablo, *Derechos y libertades, internet y tics*, Tirant lo Blanch, Valencia, 2014.

GARCÍA SAN MIGUEL RODRÍGUEZ-ARANGO, Luis, *Estudios sobre el Derecho a la Intimidad*, Editorial Tecnos S.A., Madrid, 1992.

GARCÍA, David, et. ál., *Online Privacy as a Collective Phenomenon* [en línea], http://www.sg.ethz.ch/team/people/dgarcia/

GELMAN, Robert B., *Propuesta de Declaración de los Derechos Humanos en el Ciberespacio en Internet* [en línea], 1997, http://www.arnal.es/free/info/declaracion.html

GIDDENS, Anthony, *Consecuencias de la modernidad,* Alianza Universidad, Madrid, 1994.

GINEBRA, Xavier y SAMARIO, Óscar, “Protección datos personales: ¿un derecho humano?” *Revista el Mundo del Abogado* – No. 172, agosto 2013.

GOMEZ NAVAJAS, Justa, *La protección de datos personales*, Editorial Aranzadi, Navarra, 2005.

GONZÁLEZ FERNÁNDEZ, Juan José, “El derecho a la intimidad de los derechos conexos. La perspectiva de su protección a nivel internacional, con enfoque especial al sistema latinoamericano y la situación de su reglamentación legal en México”, *Protección internacional de los Derechos Humanos*, enero 2007.

GONZÁLEZ MONTENEGRO, Rigoberto, *El hábeas data,* Edición de Defensoría del Pueblo de la República de Panamá, Panamá, 2002.

GONZÁLEZ, Graciano, *Derechos Humanos: La condición humana en la sociedad tecnológica,* Tecnos, Madrid, 1999.

GOZAÍNI, Osvaldo Alfredo (coord.), *La defensa de la intimidad y de los datos personales a través del hábeas data,* Editorial Ediar S.A. Buenos Aires, 2001.

GOZAÍNI, Osvaldo Alfredo, Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación, Rubinzal-Culzoni Editores, Santa Fé, 2002.

GREENWALD, Glenn., No place to hide, Macmillan's, New York, 2014, [versión para lector digital Kindle].

GROSS, Hyman, "The Concept of Privacy", en *New York University Law Review*, vol. 42, 1967.

GUERRA VALDIVIA, Alicia Rubí, "Redes Sociales" en NAVA GARCÉS, Alberto (coord.), *El derecho en la era digital*, ed. Porrúa, México, 2013, [versión para lector digital Kindle].

HABA MULLER, Enrique Pedro, "Derechos Humanos, Libertades Individuales y Racionalidad Jurídica", *Revista de Ciencias Jurídicas,* No. 31.

HABERMAS, Jürgen, *La inclusión del otro, estudios sobre teoría política,* Paidós, Barcelona, 1999.

HANKIN, Ron, *Invasion of privacy & the law,* Looseleaf Law Publications, New York, 2013 [versión para lector digital Kindle].

HASSEMER, Winfried y CHIRINO SÁNCHEZ, Alfredo, *El Derecho a la Autodeterminación Informativa y los Retos del Procesamiento Automatizado de Datos Personales,* Editores del Puerto s.r.l, Buenos Aires, 1997.

HERNÁNDEZ GÓMEZ, Isabel, "Introducción general a los derechos fundamentales", *Sistemas internacionales de Derechos humanos*, octubre 2002.

HERNÁNDEZ RAMOS, Mario, “El derecho al olvido en Internet como nuevo derecho fundamental en la sociedad de la información. Perspectiva constitucional española y europea”. *Quid Iuris,* Año 7, Volumen 21, junio-agosto 2013.

HERNÁNDEZ VALLE, Rubén, *Constitución Política de la República de Costa Rica. Actualizada, comentada anotada y cositas de jurisprudencia,* Editorial Juricentro, San José, 2008.

HERNÁNDEZ VALLE, Rubén, *El Derecho de la Constitución,* Editorial Juricentro, San José, Tomo II, 2004.

HERNÁNDEZ VALLE, Rubén, *Las Libertades Públicas en Costa Rica,* Editorial Juricentro, San José, 1990.

HERRÁN ORTÍZ, Ana Isabel, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de datos personales,* Ed. Dykinson, Madrid, 2003.

HERREA BRAVO, Rodolfo, “Ciberespacio, sociedad y derecho”, en RICO CARRILLO, Mariliana (coord.) *Derecho de las nuevas tecnologías,* Ediciones la Rocca, Buenos Aires, 2007.

HESS ARAYA, Christian, “Costa Rica: derecho a la privacidad y cookies”, *REDI Revista Electrónica de Derecho Informático* - No. 24, Julio 2000.

HESS ARAYA, Christian, “Libertad de comercio y acceso a Internet en Costa Rica”, *Revista de Derecho Informático,* No. 017, 1999, [en línea], http://www.alfa-redi.org/rdi-articulo.shtml?x=382

HESS ARAYA, Christian, *La dimensión jurídica del software. Naturaleza, tutela jurídica, contratos y responsabilidad,* Investigaciones Jurídicas S.A., San José, 2002.

HIGAREDA MAGAÑA, Lorena, *El derecho a la protección de datos personales la configuración del derecho al olvido,* [documento electrónico de la biblioteca Vlex].

ILLESCAS ORTÍZ, Rafael, *Derecho del comercio internacional y de la contratación electrónica,* Investigaciones Jurídicas S.A., San José, 2013.

JELLINEK, Georg, *La declaración de los derechos del hombre y el ciudadano,* traducción de CARBONEL, Miguel, Instituto de Investigaciones Jurídicas, Segunda Edición, México, 2003, [en línea], http://biblio.juridicas.unam.mx/libros/libro.htm?l=976

JINESTA LOBO, Ernesto, "Control de convencionalidad ejercido por los Tribunales y Salas Constitucionales", en FERRER MAC-GREGOR, Eduardo (coord.), *El control difuso de constitucionalidad,* Fundap, México, 2012, [en línea], http://www.ernestojinesta.com/

JOINSON, Adam y PIWEK, Lukasz, "Technology and Behaviour Change: For good and evil", New York, *Social impact of technology*, STI Press, Agosto 2013, [en línea], http://www.joinson.com/home/pubs/joinson_piwek.pdf

KLEINSTEUBER, Hans, "El surgimiento del ciberespacio: la palabra y la realidad" en VIDAL BENEYTO, José (ed.), *La ventana global,* Taurus, Madrid, 2002.

KOMMERS, Donald, "The Constitutional Jurisprudence of the Federal Republic of Germany", 3era ed., Duke University Press, 2012.

KONVITZ, Milton R., "Privacy and the Law: a Philosophical Prelude", *31 Law & Contemp.*, Probos, 1966.

LEINER, Barry y *et. ál*., "Breve historia de Internet", *Internet Society,* [en línea], http://www.internetsociety.org/es/breve-historia-de-internet#f1

LEMAÎTRE PICADO, Roberto, *Manual sobre delitos informáticos para la ciber-sociedad costarricense*, Investigaciones Jurídicas S.A, San José, 2011.

LEVINAS, Emmanuel, *Humanismo del otro hombre,* Siglo XXI, Sexta Edición, México-Madrid, 2006.

LIMA TORRADO, Jesús y ROVETTA KLYVER, Fernando, "Hipertexto y Derecho. Comunicación al III Congreso Iberoamericano de Informática Jurídica. Nuevas tecnologías y Libertades", Universidad Nacional de Educación a Distancia, Recogido luego en *Informática y Derecho*, Mérida, 1992.

LIMA TORRADO, Jesús, "Globalización y crisis de las garantías de los derechos humanos en A Distancia", vol. 19, No. 2, Editorial Invierno, Madrid, 2002.

LIMA TORRADO, Jesús, *El pensamiento único y su incidencia ideológica sobre el sistema de derechos humanos Comunicación al III Congreso Católicos y Vida Pública. Retos de la Nueva Sociedad de la Información,* Madrid, 2001, [en línea], http://www.ceu.es/fnd/jesus%20lima%20torrado.pdf

LIMA TORRADO, Jesús, *Globalización y derechos humanos en Anuario de Filosofía del Derecho,* Editorial Nueva Época, Tomo XVII, Madrid, 2000.

LLÁCER MATACÁS, María Rosa, *Protección de datos personales en la sociedad de la información y la vigilancia,* Editorial La Ley, Madrid, 2011.

LÓPEZ DIAZ, Elvira, *El derecho al honor y l derecho a la intimidad*, Ed. Dykinson, Madrid, 1996.

LÓPEZ GUERRA, L., ESPÍN TEMPLADO, E., GARCÍA MORRILLO, J., PÉREZ TREMPS, P., y SATRÚSTEGUI, M., *Derecho Constitucional,* Tirant lo Blanch, 2 vols., 9ª ed., Valencia, 2013, [versión para lector digital Kindle].

LÓPEZ JIMÉNEZ, David, "Los códigos de conducta como solución idónea frente a la elevada desprotección de la privacidad en Internet", Universidad de los

Andes, *Revista de derecho, comunicaciones y nuevas tecnologías GECTI*, número 5, junio 2011.

LÓPEZ JIMÉNEZ, David, “Los códigos tipo como instrumento para la protección de la privacidad en el ámbito digital: apreciaciones del derecho español”, *Revista de Estudios Constitucionales* – No. 2-2013, noviembre, 2013.

LÓPEZ LUNA, Paulo, "El derecho a la protección de datos personales", *El mundo del abogado,* enero 2013.

LOSANO, Mario G., PÉREZ LUÑO, Antonio Enrique y GUERRERO MATEUS, Ma. Fernanda, *Libertad informática y leyes de protección de datos personales,* Centro de estudios constitucionales, Madrid, 1989.

LUCAS MURILLO DE LA CUEVA, Pablo, El derecho a la autodeterminación informativa. La protección de datos personales frente al uso de la informática, Editorial Tecnos, Madrid, 1990.

LUCAS MURILLO DE LA CUEVA, Pablo, *El derecho a la autodeterminación informativa. La protección de datos personales frente al uso de la informática,* Editorial Tecnos, Madrid, 1990.

LYON, David, *El ojo electrónico. El auge de la sociedad de la vigilancia*, Madrid, Alianza Editorial, 1995.

MACEIRAS, Manuel, “Tecnociencia y política de derechos humanos”, en GONZALEZ, Graciano, *Derechos Humanos: La condición humana en la sociedad tecnológica,* Editorial Tecnos, Madrid, 1999.

MACHLUP, Fritz, *The production and distribution of knowledge in the United States,* Princeton University, New Jersey, 1971.

MADRID CONESA, Fulgencio, *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984.

MAIER, Julio B.J., *Derecho Procesal,* Tomo I, 2ª ed., Buenos Aires, 1996.

MARÍN ALONSO, Inmaculada, "El correo electrónico como manifestación del artículo 18.3 CE en el ámbito de la empresa: la supervivencia de la configuración del derecho pese al poder de dirección del empresario", en PÉREZ ROYO, Javier y otros, *Derecho Constitucional para el Siglo XXI,* Editorial Aranzadi, Tomo I, Navarra, 2006.

MARITAIN, Jacques, *Humanismo Integral,* Primera Edición, París, 1936.

MARTÍN MORALES, Ricardo, *El régimen constitucional del secreto de las comunicaciones,* Editorial Civitas, Madrid, 1995.

MARTÍNEZ USERO, José Ángel y LARA NAVARRA, Laura, *La accesibilidad de los contenidos web,* Editorial UOC, Cataluña, 2006.

MARTÍNEZ, Matilda Susana, *Hábeas data financiero,* Ediciones de la República, Buenos Aires, 2009.

MASUDA, Yoneji, *La sociedad informatizada como sociedad pos-industrial,* Fundescos Tecnos, Madrid, 1984.

MATTELART, Armand, *La mundialización de la comunicación,* Editorial Paidós, Barcelona, 1998.

MIGUEL CASTAÑO, Adoración, "Libertad de información y derecho de intimidad: medios para garantizarla. Incidencia en el ámbito de la estadística", REDUC, número 12, septiembre de 1986.

MILLER, Arthur, "The Assault on Privacy: Computers, Data Banks and Dossiers", *Ann Arbor, University of Michigan Press*, 1971.

MIRANDA ALCÁNTARA, Manuel Iván, *Informática, intimidad y protección de Bases de datos* [en línea], http://www.teleley.com/articulos/art-miranda.pdf

MONGE, Ricardo, y CHACON Federico, *La Brecha Digital en Costa Rica. Acceso y uso de las Tecnologías de la Información y Comunicaciones (TIC's),* [en línea], http://www.caatec.org/CAATEC/publicaciones/crdigital/CR_Digital_1.pdf

MONTAÑÉS PARDO, Miguel Ángel, *La intervención de las comunicaciones,* Pamplona, Editorial Aranzadi, 2000.

MONTERO AROCA, Juan, La intervención de las comunicaciones telefónicas en el proceso penal: un estudio jurisprudencial. Valencia, Ed. Tirant Lo Blanch, 1999.

MORAIS, Sabrina, "La protección de datos en el ámbito español y el panorama jurídico brasileño", *Revista Eletrônica de Direito Processual* - No. 1-2007, diciembre, 2007.

MORALES PRATS, Fermín, "Protección penal de la intimidad, frente al uso ilícito de la informática en el código penal de 1995", en *Cuadernos de Derecho Judicial*, Escuela Judicial, Consejo General del Poder Judicial. C.G.P.J. No. XI, "Delitos contra la libertad y Seguridad", Madrid, 1996.

MORALES PRATS, Fermín, *La tutela penal de la intimidad: privacy e informática,* Barcelona, 1984.

MORÁN MARTÍN, Remedios, "Los derechos sobre las cosas. El derecho de propiedad y derecho de posesión", en *Historia del Derecho Privado, Penal y Procesal*, Editorial Universitas, Tomo I, Parte teórica, 2002.

MORÓN LERMA, Esther, *Internet y derecho penal: hacking y otras conductas ilícitas en la red,* Editorial Aranzadi, Madrid, 1999.

MOSCOSO SEGARRA, Alejandro, "Las intervenciones telefónicas y el derecho a la intimidad", *Gaceta Judicial,* febrero, 2014, [documento electrónico de Vlex].

MUÑOZ ALVARADO, Ma. Daniela y NICARAGUA NICARAGUA, Rosa, “Un acercamiento a la brecha digital en Costa Rica desde el punto de vista del acceso, la conectividad y la alfabetización digital” en Revista electrónica publicada por la Escuela de Bibliotecología y Ciencias de la Información, UCR, vol. 4, No. 1, 2014, [en línea], http://revistas.ucr.ac.cr/index.php/eciencias/article/view/12866/12328

MUÑOZ CAMPOS, Mercedes y SOTO ARROYO, Hannia, *Derecho de Autodeterminación Informativa,* Editorial Jurídica Continental, San José, 2005.

MUÑOZ MACHADO, Santiago, *La regulación de la red,* Taurus, Madrid, 2000.

MUÑOZCANO ETERNOD, Antonio, *El derecho a la intimidad frente al derecho a la información,* Porrúa, México D.F., 2010.

MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis, *El derecho a la autodeterminación informativa,* Fundación Coloquio Jurídico Europeo, Madrid, 2009.

NÁJERA MONTIEL, Javier, “El Thelos de la protección de los datos personales ante el derecho al acceso a la información”, *Ius Humani, Revista de Derecho,* vol. 1 (2008/2009), enero, 2008.

NAVA GARCÉS, Alberto (coord.), *El derecho en la era digital,* ed. Porrúa, México, 2013, [versión para lector digital Kindle].

NAVA GARCÉS, Alberto, “La regulación de las nuevas tecnologías”, en *El mundo del abogado,* 2012.

NEBRERA GONZÁLEZ, Montserrat (coord.), *Intimidad y seguridad: dos conceptos y un conflicto*, Associació Isegs per a la Promoció dels Estudis sobre la Governabilitat, Barcelona, 2002.

NISSENABAUM, Helen, *Privacidad amenazada, tecnología, política y la integridad de la vida social,* Océano, México, 2011.

O'DONNELL, Guillermo, “La irrenunciabilidad del Estado de Derecho”, en *Revista Instituciones y Desarrollo,* No. 8 y 9, Institut Internacional de Governabilitat de Catalunya, Còrsega, Barcelona, 2001.

ORNELAS NÚÑEZ, Lina Gabriela e HIGUERA PÉREZ, Melissa, “La autorregulación en materia de protección de datos personales: la vía hacia una protección global”, *Revista de Derecho, Comunicaciones y Nuevas Tecnologías* - No. 9, junio, 2013.

ORTEGA MARTÍNEZ, Jesús, *Sociedad de la información y derechos humanos de cuarta generación. Un desafío inmediato para el derecho constitucional,* Derecho Constitucional, Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados, [en línea], http://www.bibliojuridica.org/libros/libro.htm?l=1510

ORTÍ VALLEJO, Antonio, *Derecho a la intimidad e informática. Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada*, Editorial Comares, Granada, 1984.

PABLOS PONS, Juan, *Las tecnologías de la información y la comunicación: un punto de vista educativo* [en línea], http://www.ucm.es/info/multidoc/multidoc/revista/num8/jpablos.html

PADILLA, Miguel M., *Bancos de datos y acción de hábeas data,* Abeledo-Perrot, Buenos Aires, 2001.

PARDO LÓPEZ, María, “No sólo protección de datos personales en Internet: de los conceptos jurídicos y libros, las categorías mutantes y otras evoluciones en

curso", En VALERO TORRIJOS, Julián (coord.), La protección de los datos personales en Internet ante la innovación tecnológica, Aranzadi, Madrid, 2013.

PAREJO ALFONSO, Luciano, "El derecho fundamental a la intimidad", IUS ET PRAXIS, Lima, *Revista de la Universidad de Lima,* No. 21-22, 1993.

PAREJO ALFONSO, Luciano, *El Derecho Fundamental a la intimidad. Problemas Actuales de los Derechos Fundamentales*, Madrid, España, 1994.

PATIÑO CRUZ, (Silvia), *et. ál.*, *El recurso de amparo en Costa Rica,* Editorama S. A., San José, 2008.

PECES-BARBA, Gregorio, "La Universalidad de los Derechos Fundamentales", en *Revista del Movimiento por la Paz, el Desarme y la Libertad,* 1993.

PECES-BARBA, Gregorio, *Curso de Derechos Fundamentales. Teoría General,* Primera reimpresión, Imprenta Nacional del Boletín Oficial del Estado, Universidad Carlos III de Madrid, Madrid, 1999.

PECES-BARBA, Gregorio, *Derechos Fundamentales,* Universidad de Madrid, Madrid, 1983.

PECES-BARBA, Gregorio, *La Constitución y los derechos,* Universidad Externado, Bogotá, 2006.

PEPPET, Scott R., "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", 93 *Texas Law Review*, no. 85, 2014, [en línea], http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf

PÉREZ LUÑO, Antonio Enrique, "Bioética e intimidad. La tutela de los datos personales biomédicos", en MARCOS DEL CANO, Ana María, *Bioética, Filosofía y Derecho,* Aldaba, No. 32. Servicio de Publicaciones del Centro Uned-Melilla, 2004.

PÉREZ LUÑO, Antonio Enrique, “Impactos sociales y jurídicos de Internet” en *Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología,* No. 1, 1998, [en línea], http://www.argumentos.us.es/numero1/bluno.htm

PÉREZ LUÑO, Antonio Enrique, “La protección de la intimidad frente a la informática en la Constitución Española de 1978”. *Derechos económicos, sociales y culturales: para una integración histórica y doctrinal de los derechos humanos: actas de las IV Jornadas de Profesores de Filosofía del Derecho,* Murcia, 1981, [en línea], http://www.cepc.es/rap/Publicaciones/Revistas/3/REPNE_009_059.pdf

PÉREZ LUÑO, Antonio Enrique, “La protección de la intimidad frente al informática en la constitución española de 1978”. *REP.*, No. 9, mayo-junio, 1979.

PÉREZ LUÑO, Antonio Enrique, “Los Derechos Humanos en la Sociedad Tecnológica”, *Cuadernos y Debate,* en vol. *Libertad Informática y Protección de Datos Personales,* Centro de Estudios Constitucionales, Madrid, 1999.

PÉREZ LUÑO, Antonio Enrique, *Cibernética, Informática y Derecho,* Publicaciones del Real Colegio de España, Bolonia, 1976.

PÉREZ LUÑO, Antonio Enrique, *Derechos Humanos, Estado de Derecho y Constitución,* Editorial Tecnos S.A., Madrid, 5ª ed., 1995.

PÉREZ LUÑO, Antonio Enrique, *La tercera generación de derechos,* Thomson, Navarra, 2006.

PÉREZ LUÑO, Antonio Enrique, *Los derechos humanos en la sociedad tecnológica,* Editorial Universitas S. A., Madrid, 2012.

PFANDER, James E., *The Story of Bivens v. Six Unknown-Named Agents of the Federal Bureau of Narcotics*, Northwestern University School of Law, 2009, [en línea],

http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1188&context=facultyworkingpapers

PICADO, Sonia, *La fundamentación histórica, filosófica y jurídica de los Derechos Humanos,* [en línea], http://www.iidh.ed.cr/

PIERINI Alicia*, Hábeas data: derecho a la intimidad*. Buenos Aires. Argentina. Universidad. 2002.

PIERINI, Alicia, LORENCES Valentín, TORNABENE, María Inés, *Hábeas data. Derecho a la intimidad,* 2ª ed., Editorial Universidad, Buenos Aires, 2002.

PORAT, Marc, *The information economy: definition and measurement*, Department of Commerce, United States, 1977.

PROSER, William L., "Privacy", *California Law Review,* vol. 48, No. 3, 1960, [en línea], http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3157&context=californialawreview

PUCCINELLI, Óscar R., *Derecho Procesal Constitucional: Hábeas data, Protección de datos personales,* Editorial Rubinzal – Culzoni, Buenos Aires, 2002.

PUCCINELLI, Óscar R., *El habeas data en Indoiberoamérica,* Editorial Temis, Bogotá, 1999.

PUCCINELLI, Óscar R., *Protección de datos de carácter personal,* Editorial Astrea de Alfredo y Ricardo Depalma SRL, Buenos Aires, 2004.

PUENTE DE LA MORA, Ximena, "Privacidad de la información personal y su protección legal en Estados Unidos", *Consumo & amp; Legal* - No. 7, febrero, 2007.

QUÉAU, Philippe, "La sociedad de la Información y el bien público mundial" en VIDAL BENEYTO, José (ed.), *La ventana global,* Taurus, Madrid, 2002.

QUESADA MORA, Juan Gerardo, *Temas sobre Derechos Fundamentales y Constitucionales,* Investigaciones Jurídicas S. A., San José, 2004.

REBOLLO DELGADO, Lucrecio, *El derecho fundamental a la intimidad,* ed. Dykinson, Segunda edición, Madrid, 2005.

REYES VALENZUELA, Santa Matilde, *Protección de datos de carácter personal. Flujo de datos de carácter personal en un mundo globalizado,* Editorial académica española, Madrid, 2013.

RIASCOS GÓMEZ, Libardo Orlando, "El delito informático contra la intimidad de las personas: una visión constitucional y penal", *Ponencia presentada en el Congreso Latinoamericano de Derecho Informático*, Buenos Aires, 2004.

RIASCOS GÓMEZ, Libardo Orlando, "El derecho a la intimidad, visión iusinformática y el delito de los datos personales", *Tesis Doctoral,* Universidad de Lleida, España, 1999.

RIBAS, Javier, *"*Aspectos legislativos de las autopistas de la información*:* Delitos en Internet"*,* en *Jornadas Profesionales Informat- 96,* Barcelona, octubre, 1996.

RICO CARRILLO, Mariliana (coord.), *Derecho de las nuevas tecnologías,* Ediciones la Rocca, Buenos Aires, 2007.

RICO CARRILLO, Mariliana, "Las implicaciones de Facebook en el derecho al honor, la intimidad personal y familiar y de la propia imagen", *Revista de Contratación Electrónica* - No. 117, enero 2012.

RIVERA SANCLEMENTE, María del Rosario, "La protección de datos en el entorno laboral", Universidad de los Andes, Revista de derecho, comunicaciones y nuevas tecnologías GECTI, número 7, junio 2012.

ROBERTO SOBRINO, Waldo Augusto, “Las cookies y el spam (y la violación de la privacidad y la intimidad)”, *REDI Revista Electrónica de Derecho Informático* - No. 35, Junio 2001.

RODRÍGUEZ LAINZ, José Luis, *Intervención Judicial en los Datos de Tráfico de las Comunicaciones,* Editorial Bosch S.A., Barcelona, 2003.

RODRÍGUEZ MERINO, José M., “La confidencialidad de datos sanitarios” en *Ética y derechos humanos en la era biotecnológica,* febrero 2009.

RODRÍGUEZ RUÍZ, Blanca, El secreto de las comunicaciones (Tecnología e intimidad), McGraw Hill, Madrid, 1997.

ROSA VELÁZQUEZ, Luis D., “Panorama General del Derecho a la Intimidad”, en *Revista Jurídica Universidad de Puerto Rica,* vol. 72.4, 2002.

ROSARIO, Jimmy, “La tecnología de la información y la comunicación (TIC). Su uso como herramienta para el fortalecimiento y el desarrollo de la educación virtual”, 2005, disponible en *Archivo del Observatorio para la CiberSociedad,* [en línea], http://www.cibersociedad.net/archivo/articulo.php?art=218

ROSEN, Jeffrey, “The Right to Be Forgotten”, en 64 *Stanford Law Review*, 13 de febrero, 2012, [en línea], http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

RUBIRA GARCÍA, Rainer, *Hacia una regulación ética del ciberespacio desde la Unesco,* [Biblioteca Vlex].

RUÍZ MARCO, Francisco, *Los delitos contra la intimidad,* Editorial Colex, Madrid, 2001.

RUÍZ MIGUEL, Carlos, “Derechos constitucionales, fiscalidad e Internet: necesidad de una reformulación de conceptos tradicionales”, en *Cuadernos*

Constitucionales de la Cátedra Fadrique Furió Ceriol, Universitat de València, No. pp. 47-56.

RUÍZ MIGUEL, Carlos, *La configuración constitucional del derecho a la intimidad, Madrid, España,* Ed. Tecnos, 1995.

RUSTAD, Michael L., *Global Internet law*, editorial West, segunda edición, Minnesota, 2013, [versión para lector digital Kindle].

SAGARDOY BENGOECHEA, J. A., *Los derechos fundamentales y contrato de trabajo,* Civitas, Madrid, 2005.

SALDAÑA, María Nieves, "La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de información personal en los Estados Unidos", *Revista Aucaria*, vol. 9, num. 18, 2007.

SÁNCHEZ CARAZO, Carmen, "La protección de datos personales de las personas vulnerables", en *Anuario Facultad de Derecho*, Universidad de Alcalá II, 2009, [en línea], http://dspace.uah.es/dspace/handle/10017/6443

SÁNCHEZ DEL CASTILLO, Vilma, *La sociedad de información y sus servicios,* Editorial Investigaciones Jurídicas S. A. San José, 2014.

SÁNCHEZ LÓPEZ, David, "El acceso a Internet: la disputa", *Foro jurídico* - No. 113, febrero 2013.

SANZ DE LAS HERAS, Jesús, *Abusos en el correo electrónico* [en línea], http://www.ucm.es/info/dinforma/activi/libro/9.html

SAURA, Nuria, "La protección de la libertad de expresión en Internet: análisis de la jurisprudencia del Tribunal Europeo de Derechos Humanos", en *El control de los Cibermedios,* mayo, 2014.

SCHLAIN, Natalia Beatriz, *Internet y el derecho a la intimidad,* Editorial académica española, Madrid, 2012.

SCHNEIER, Bruce, *Data and Goliath. The hidden battles to collect your data and control your world,* Editorial W.W. Norton & Company, New York, London, 2015, [versión para lector digital Kindle].

SCHWARTZ, Paul M. y SOLOVE, Daniel J., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" *New York University Law Review*, vol. 86, New York, 5 de diciembre, 2011, [en línea], http://ssrn.com/abstract=1909366

SCHWARTZ, Paul M., "Internet, Privacy and the State", en *Connecticut Law Review*, vol. 32, 2000.

SCHWARTZ, Paul M., "Privacy and Democracy in Cyberspace", en *Vanderbilt Law Review*, vol. 52, 1999.

SCIENTIKA, "Los límites entre la privacidad y la tecnología", en *Foro jurídico* - No. 125, febrero 2014.

SOLOVE, Daniel J. y HARTZOG, Woodrow, "The FTC and the New Common Law of Privacy", en 114 *Columbia Law Review* 583 (2014), GWU *Legal Studies Research Paper* No. 2013-120, GWU *Law School Public Law Research Paper* No. 2013-120, Agosto, 2013, [en línea], http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913

SOLOVE, Daniel J. y SCHWARTZ Paul M., *Privacy Law Fundamentals,* IAPP Publications, 3era edición, New Haven, 2015.

SOLOVE, Daniel J. y SCHWARTZ Paul M., *Privacy, information and technology,* Wolters Kluwer Law, 3era edición, Maryland, 2011.

SOLOVE, Daniel J., *Nothing to hide: the false tradeoff between privacy and security,* Yale University Press, New Haven and London, 2013.

SOLOVE, Daniel J., *The digital person. Technology and privacy in the information age,* New York University Press, New York and London, 2004.

SOLOVE, Daniel J., *Understanding privacy,* President and fellows of Harvard College, Estados Unidos, 2008.

SOMA John T., RYNERSON Stephen D. y KITAEV Erica, *Privacy Law*, Editorial West, Minnesota, 2014, [versión para lector digital Kindle].

STAFF WILSON Mariblanca, *Mujer y derechos humanos,* KO'AGA ROÑE'ETA se.viii, Panamá, 1998. [en línea], http://www.derechos.org/koaga/viii/staff.html

STARCK, Christian, *Jurisdicción Constitucional y Derechos Fundamentales,* Dykinson, Madrid, 2011.

SUBIZA PÉREZ, Ignacio, *La protección de datos y sus mundos. La construcción del derecho a la protección de datos personales como un derecho autónomo,* Editotial DAPP Publicaciones Jurídicas, Madrid, 2009.

TAPIA BUENO, Seidy Galina, "La Protección Jurídica de los Datos Biométricos en la Comunidad Europea", agosto, 2005, [en línea], http://www.buscalegis.ufsc.br/revistas/files/anexos/5548-5540-1-PB.htm

TELLEZ, Julio, *Derecho Informático*, 3ra Ed, McGraw Hill/Interamericana Editores S.A., México, 2004.

TORNABENE, Inés, "Privacidad e intimidad: la protección legal de la información personal en la República Argentina", en AMOROSO FERNÁNDEZ, Y., (dir.), *Género, Código de Juventud: construir sociedades más justas e inclusivas*, Unión Nacional de Juristas de Cuba, 2014, pp. 85-101.

TRONCOSO REIGADA, Antonio, "El derecho el olvido en Internet a la luz de la propuesta de reglamento general de protección de datos personales de la

Unión Europea", Universidad de los Andes, *Revista de derecho, comunicaciones y nuevas tecnologías GECTI,* número 8, diciembre 2012.

UGARTE CATALDO, José Luis, "Privacidad, trabajo y derechos fundamentales", en *Estudios Constitucionales*, año nueve, No. 1, 2011, pp. 13 -36.

UICICH, Rodolfo Daniel, *Los bancos de datos y el derecho a la intimidad,* Editorial Ad-Hoc S.R.L. Buenos Aires, 1999.

URBANO CASTRILLO, Eduardo, *El derecho al secreto de las comunicaciones*, Madrid, ed. La Ley 2011.

VALERO TORRIJOS, Julián (coord.), La protección de los datos personales en Internet ante la innovación tecnológica, Aranzadi, Madrid, 2013.

VARELA FERRÍO, José, *La brecha digital en España estudio sobre la desigualdad postergada,* Comisión Ejecutiva Confederal de UGT, Madrid, 2015, [en línea], http://www.ugt.es/Publicaciones/BRECHADIGITAL_WEB.pdf

VÁZQUEZ RUANO, Trinidad, "La tutela de la información personal y el uso de las redes sociales" en *Universitas, Revista de Filosofía, Derecho y Política,* N°15. Enero 2012, [en línea], http://universitas.idhbc.es/n15/15-06.pdf

VERA SANTOS, José Manuel, "Derechos fundamentales, Internet y nuevas tecnologías de la información y de la comunicación" en GARCÍA MEXÍA, Pablo (dir.), *Principios de Derecho de Internet,* Tirant lo Blanch, Valencia, 2ª ed., 2005.

VILLAHERMOSA IGLESIAS, Alfonso, "Algunos apuntes técnicos y jurídicos sobre los principales protocolos de seguridad utilizados en Internet" en *Revista de Derecho Informático,* 2004. [en línea] http://www.alfa-redi.org/rdi-articulo.shtml?x=1225

VILLATE, Javier, *La libertad de expresión en Internet: retos y amenazas* [en línea], http://www.une.edu.ve/~iramirez/te1/censura_internet.html

VILLATORO, Pablo y HOPENHAYN, Martín, *El derecho a la educación. Una tarea pendiente para América Latina y el Caribe,* Publicación de la Naciones Unidas, 2006, [en línea] http://www.unicef.org/mexico/spanish/Desafios_Nro3_Educacion_Ago2006(2).pdf

VV. AA. *Orígenes de la Declaración de Derechos del Hombre y del Ciudadano,* Editora Nacional, Madrid, 1984.

WARREN, Samuel D. y BRANDEIS, Louis D., "The Right to Privacy"*,* en *Harvard Law Review*, 4, 1890. [en línea], http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

WESTIN, Alan F., *Privacy and freedom*, Atheneum, New York, 1967.

WHITMAN, James. Q., "The Two Western Cultures of Privacy: Dignity versus Liberty", en *Yale Law Journal*, vol. 113, 2004.

ZAGREBELSKY, Gustavo, *El derecho dúctil. Ley, derechos, justicia,* Editorial Trotta, Décima Edición, Madrid, 2011.

2. NORMATIVA.

2.1. Tratados, Convenios Internacionales y normativa europea.

Carta de los Derechos Fundamentales de la Unión Europea

Convención Americana sobre Derechos Humanos (Pacto de San José), suscrita en Costa Rica el 7 del al 22 de noviembre de 1969, consultable en: http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

Convención Europea para la protección de los Derechos Humanos y de las libertades fundamentales, consultable en: http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/SpanishEspagnol.pdf

Convención sobre los Derechos del Niño de 1989, consultable en: http://www.unicef.org/argentina/spanish/7.-Convencionsobrelosderechos.pdf

Declaración Americana de Derechos y Deberes del Hombre, de 2 de mayo de 1948, consultable en: http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948, consultable en: http://www.un.org/es/documents/udhr/

Directiva 1995/46/CE del Parlamento Europeo y del Consejo de 24 de octubre del 1995.

Directiva 1997/66/CE, del Parlamento Europeo y del Consejo de 15 de diciembre de 1997.

Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006.

Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009.

Directiva 2009/136/CE del Parlamento Europeo y el Consejo del año 2009.

Directiva 2009/140/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009.

Pacto Internacional de Derechos Civiles y Políticos, consultable en: http://www.unhchr.ch/spanish/html/menu3/b/a_ccpr_sp.htm

Principios de Siracusa sobre las Disposiciones de Limitación y Derogación del Pacto Internacional de Derechos Civiles y Políticos, Comisión de Derechos Humanos 41º Período de sesiones, temas 18 del programa provisional, 24 de agosto de 1984, [en línea], http://www.derechos.org/nizkor/excep/siracusa84.html

Propuesta del Reglamento General de Protección de Datos de la U.E.

2.2. Constituciones.

2.2.1. Nacionales y Federales.

Carta de Derechos de Estados Unidos de América, de 3 de noviembre de 1791, en español, consultable en: http://www.archives.gov/espanol/declaracion-de-derechos.html

Constitución de los Estados Unidos de América, de 1787, en español, consultable en: http://www.archives.gov/espanol/constitucion.html

Constitución Política de Costa Rica, de 1949, consultable en: http://www.asamblea.go.cr/Centro_de_Informacion/biblioteca/Paginas/Constituci%C3%B3n%20Pol%C3%ADtica%20de%20Costa%20Rica.aspx

Constitución Política de España, de 1978, consultable en: http://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf

2.2.2. Estatales.

Constitution of the State of Alaska

Constitution of the State of California

Constitution of the State of Florida

Constitution of the State of Arizona

Constitution of the State of Montana

Constitution of the State of Hawaii

Constitution of the State of Illinois

Constitution of the State of South Carolina

Constitution of the State of Louisiana

Constitution of the State of Washington

2.3. Leyes.

2.3.1.1. Estados Unidos de América.

Bank Secrecy Act (BSA) of 1970, Pub. L. 91–508, [en línea], https://www.law.cornell.edu/uscode/text/31/5311

Cable Communications Policy Act (CCPA) of 1984, 47 U.S.C. § 551, [en línea], http://www.publicaccess.org/cableact.html

California Shine the Light Law Civil Code §§1798.83 of XX, [en línea], http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84

CAN-SPAM Act of 2003, Pub. L. No. 108-187, [en línea], https://www.law.cornell.edu/wex/inbox/can-spam_act_core_requirements

Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. § 6501–6505, [en línea], https://www.law.cornell.edu/uscode/text/15/chapter-91

Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. 103–414, [en línea], https://www.law.cornell.edu/uscode/text/18/2522

Computer Matching and Privacy Protection Act (CMPP) of 1988, 5 U.S. Code § 552ª, [en línea], https://www.law.cornell.edu/uscode/text/5/552a

Electronic Communications Privacy Act (ECPA) of 1986, 18 U.S.C. § 2510-22, [en línea], https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

Employee Polygraph Protection Act (EPPA) of 1988, 29 U.S. Code Chapter 22, [en línea], https://www.law.cornell.edu/uscode/text/29/chapter-22

Fair and Accurate Credit Transactions Act (FACT) of 2003, Pub. L. 108-159, [en línea], https://www.law.cornell.edu/cfr/text/16/602.1

Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. § 1681, [en línea], http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf

Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g, [en línea], https://www.law.cornell.edu/uscode/text/20/1232g

Foreign Surveillance Act (FISA) of 1978, 50 U.S. Code Chapter 36, [en línea], https://www.law.cornell.edu/uscode/text/50/chapter-36

Genetic Information Nondiscrimination Act (GINA) of 2007, Pub. L. 110–233, title II, § 201, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/html/PLAW-110publ233.htm

Gramm-Leach-Bliley (GLB) Act of 1999, 12 U.S.C. § 1811, [en línea], https://www.law.cornell.edu/uscode/text/12/1811

Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 [en línea], http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf

Identity Theft and Assumption Deterrence Act (ITADA) of 1996, 18 U.S. § 1028, [en línea], https://www.law.cornell.edu/uscode/text/18/part-I/chapter-47

Intelligence Reform and Terrorism Prevention Act of 2004, P. L. 108-458, [en línea], http://www.intelligence.senate.gov/laws/intelligence-reform-and-terrorism-prevention-act-2004

National Security Act of 1947, [en línea], http://www.intelligence.senate.gov/sites/default/files/laws/nsact1947.pdf

Pen Register/Trap and Trace Device (Pen/Trap), [en línea], https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206

Personal Responsibility and Work Opportunity Reconciliation Act (PRWOR) of 1996, Pub. L. 104–193, [en línea], http://www.law.cornell.edu/uscode/text/42/616&prev=search

Privacy Act (PA) of 1974, U.S.C. 5 § 552a, [en línea], http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf

Privacy Bill of Rights Act of 2015, proyecto de ley, [en línea], https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf

Privacy Protection Act (PPA) of 1980, 42 U.S. Code Chapter 21ª, [en línea], https://www.law.cornell.edu/uscode/text/42/chapter-21A

Protect America Act (PAA) of 2007, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm

Restatement (Second) of Torts, §§ 652A-E, [en línea], http://www.tomwbell.com/NetLaw/Ch05/R2ndTorts.html

Right to Financial Privacy Act (RFPA) of 1978, 12 U.S. Code Chapter 35, [en línea], https://www.law.cornell.edu/uscode/text/12/chapter-35

Telephone Consumer Protection Act (TCPA) of 1991, 47 U.S.C. § 227, [en línea], https://transition.fcc.gov/cgb/policy/TCPA-Rules.pdf

USA FREEDOM Act of 2015, H.R. 2048, the "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015", [en línea], https://www.congress.gov/bill/114th-congress/house-bill/2048/text

USA-PATRIOT Act (USAPA) of 2001, Pub. L. No. 107-56, [en línea], http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

Video Privacy Protection Act (VPPA) of 1988, 18 U.S.C. §§ 2710-11, [en línea], https://www.law.cornell.edu/uscode/text/18/2710

Video Voyeurism Prevention Act (VVPA) of 2004, Pub. L. 108–495, [en línea], https://www.law.cornell.edu/uscode/text/18/1801

2.3.1.2. España.

El texto del proyecto de reforma de la Ley de Enjuiciamiento Criminal, puede ser consultado en: http://www.ub.edu/dpenal/recursos/doc_legislacio/LECr_anteproyecto_y_otras_2014.pdf

Ley 2/2011, de 4 de marzo, de economía sostenible (BOE núm. 55 de 5-3-2011, pp. 25033-25235). Consultable en: http://www.boe.es/boe/dias/2011/03/05/pdfs/BOE-A-2011-4117.pdf

Ley de Enjuiciamiento Criminal (LECrim).

Ley de servicios de la sociedad de la información y de comercio electrónico 34/2002, reformada por el Real Decreto-ley 13/2012, de 30 de marzo.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298, de 14-12-1999, pp. 43088-43099). Consultable en: https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal

2.3.1.3. Costa Rica.

Código Penal de Costa Rica, Ley No. 4573 de 15 de noviembre de 1970.

Ley No. 8968, Ley de protección de la persona frente al tratamiento de sus datos personales.

Ley sobre el registro, secuestro y examen de documentos privados e intervención de las comunicaciones, Ley No. 7425, de 09 de agosto de 1994, [en línea], 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

2.4. Otros instrumentos legales.

Declaración de Principios para la primera fase de la Cumbre Mundial sobre la Sociedad de la Información, Ginebra, 10- 12 de diciembre 2003, [en línea], http://www.itu.int/wsis/docs/geneva/official/dop-es.html

Decreto Ejecutivo No. 37554 del 30 de octubre de 2012, Reglamento a la Ley de Protección de la persona frente al tratamiento de sus datos personales.

Dictamen del Supervisor Europeo de Protección de Datos de 16 de octubre de 2010, No. 2010/C 280/01, Bruselas, [en línea], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:280:0001:0015:ES:PDF

Executive Order 12333 of 1981, [en línea], http://www.archives.gov/federal-register/codification/executive-order/12333.html

Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado mediante Real Decreto 1720/2007.

3. JURISPRUDENCIA.

3.1. Resoluciones del Parlamento Europeo.

Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior (2013/2188(INI)).

Resolución del Parlamento Europeo, de 29 de octubre de 2015, sobre el seguimiento de la Resolución del Parlamento Europeo, de 12 de marzo de 2014, relativa a la vigilancia electrónica masiva de los ciudadanos de la UE (2015/2635(RSP)).

3.2. Corte Europea de Derechos Humanos[849].

Weber and Saravia v. Germany de 2006

Malone v. UK de 1984

S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 41, 4 December 2008

Sciacca v. Italy, no. 50774/99, § 29, ECHR 2005-I.

P.G. and J.H. v. the United Kingdom, no. 44787/98, §§ 59-60, ECHR 2001-IX.

---

[849] Corte Europea de Derechos Humanos. Consultable en: http://www.echr.coe.int/Pages/home.aspx?p=home&c=

Peck v. the United Kingdom, no. 44647/98, §§ 60-63, ECHR 2003-I.

Uzun v. Germany no. 35623/05, 2 September 2010.

Airey v. Ireland, 9 October 1979, § 32, Series A no. 32.

X and Y v. the Netherlands, 26 March 1985.

August v. the United Kingdom (dec.), no. 36505/02, 21 January 2003.

M.C. v. Bulgaria, no. 39272/98, § 150, ECHR 2003-XII

K.U. v. Finland (no. 2872/02, § 43, 2 December 2008

Amann v. Switzerland [GC], no. 27798/95, § 69, ECHR 2000-II

Gaskin v. the United Kingdom, 7 July 1989.

Niemietz v. Germany, 16 December 1992.

Halford v. the United Kingdom, 25 June 1997.

Copland v. the United Kingdom, no. 62617/00, § 30, ECHR 2007-IV

.....
.....

Rotaru v. Romania [GC], no. 28341/95, ECHR 2000-V

Liberty and Others v. the United Kingdom, no. 58243/00, § 62, 1 July 2008.

Klass and Others v. Germany, 6 September 1978, §§ 49-50, Series A no. 28.

3.3. Tribunal de Justicia de la Unión Europea.

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 9 de noviembre de 2010, en los asuntos acumulados, Volker und Markus Schecke C-92/09 y Hartmut Eifert Land Hessen C-93/09, consultable en:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=152652

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12, consultable en: http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=2&dir=&occ=first&part=1&text=privacidad&doclang=ES&cid=278502#ctx1

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera), de 17 de septiembre de 2015, en el asunto C-85/14, consultable en: http://curia.europa.eu/juris/document/document.jsf?text=privacidad&docid=167948&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=278502#ctx1

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14, consultable en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=240406

3.4. Corte Interamericana de Derechos Humanos.

Almonacid Arellano y otros c/. Chile, de 26 de septiembre de 2006.

Cabrera García y Montiel Flores c/. México, de 26 de noviembre de 2010.

Gelman c/. Uruguay, de 24 de febrero de 2011.

Trabajadores Cesados del Congreso c/. Perú, de 24 de noviembre de 2006.

Tristán Donoso c/. Panamá, de 27 de enero de 2009.

3.5. Corte Suprema de los Estados Unidos de América y Cortes Supremas de los Estados.

Bivens v. Six Unknown Named Agents 403 U.S. 388 (1971).

Cain v. Hearst Corp., 878 S.W.2d 577 (Tex. 1994).

Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 864–65, ND Cal. 2011.

Daniels v. JP Morgan Chase Bank, NA, No. 22575/09, 2011.

Eisenstadt v. Baird 405 U.S. 438 (1972).

Griswold v. Connecticut 381 EE.UU. 479 (1965).

Griswold v. Connecticut 381 U.S. 479 (1965).

Hester v. United States 265 U.S. 57 (1924).

Lake v. Wal-Mart, 582 N.W.2d 231, (1998).

Lawrence v. Texas 539 U.S. 558 (2003).

Loeffler v. Ritz-Carlton Hotel Co., No. 2:06-CV-0333-ECR-LRL.

NAACP v. Alabama, 357 U.S. 449, (1958).

Nixon v. Fitzgerald 457 U.S. 731 (1982).

Renwick v. News and Observer Pub. Co., 312 S.E.2d 405 (N.C. 1984).

Roe v. Wade 410 U.S. 113 (1973).

Shelton v. Tucker, 364 U.S. 479 (1960).

Sullivan v. Pulitzer Broadcasting Co., 709 S.W.2d 475 (Mo. 1986).

Verizon v. FCC, 740 F.3d 623, D.C. Cir. Jan. 14, (2014).

Whalen v. Roe 429 U.S. 589 (1977)

3.6. Tribunal Constitucional de España.

STC, Sección Segunda. Auto 257/1985, de 17 de abril de 1985.

STC, Sala Segunda. Sentencia 168/1986, de 22 de diciembre de 1986.

STC, Sección Cuarta. Auto 642/1986, de 23 de julio de 1986.

STC, Sala Segunda. Sentencia 231/1988, de 2 de diciembre de 1988.

STC, Sala Primera. Sentencia 254/1993, de 20 de julio de 1993.

STC, Pleno. Sentencia 341/1993, de 18 de noviembre de 1993.

STC, Sala Primera. Sentencia 143/1994, de 9 de mayo de 1994.

STC, Sala Segunda. Sentencia 94/1998, de 4 de mayo de 1998.

STC, Sala Segunda. Sentencia 144/1999, de 22 de julio de 1999.

STC, Sala Primera. Sentencia 202/1999, de 8 de noviembre de 1999.

STC, Pleno. Sentencia 292/2000, de 30 de noviembre de 2000.

STC, Sala Primera. Sentencia 70/2002, de 3 de abril de 2002.

STC, Sala Primera. Sentencia 123/2002, de 20 de mayo de 2002.

3.7. Sala Constitucional de Costa Rica.

SSC número 2013-10712 de las 11:31 hrs. del 8 de agosto de 2013.

SSC número 2012-3477 de las 14:30 hrs. del 31 de julio de 2012.

SSC número 6776-94 de las 14:57 hrs. del 22 de noviembre de 1994.

SSC número 2014-11715.

SSC número 08-9690 de las 15:12 hrs. del 30 de julio de 2008.

SSC número 3013-94 de las 15:03 del 22 de junio de 1994.

SSC número 0627-93 de las 16:03 hrs. del 08 de febrero de 1993.

SSC número 1261-90 de las 15:30 hrs. del 10 de setiembre de 1990.

SSC número 1999-04847 de las 16:27 hrs. del 22 de junio de 1999.

SSC número 05802-99 de las 15:36 hrs. del 27 de julio de 1999.

SSC número 2007-17097 de las 9:29 hrs. del 23 de noviembre de 2007.

SSC número 2007-15605 de las 17:35 hrs. del 11 de diciembre de 2007.

SSC 2013-013326 de las 9:05 hrs. del 4 de octubre de 2013.

SSC número 2014-4035 de las 11:00 hrs. del 21 de marzo de 2014.

SSC 95-3195

Sala Tercera de la Corte Suprema de Justicia No. 2012-01383, de las 9:22 hrs. del 31 de agosto de 2012.

SSC número 2012-6628 de las 11:42 hrs. del 22 de junio de 2012.

SSC número 2012-13097 de las 11:00 hrs. del 18 de setiembre de 2012.

SSC número 2012-7118 de las 9:30 hrs. del 29 de junio de 2012.

SSC número 2012-3712 de las 9:05 hrs. del 16 de marzo de 2012.

3.8. Consejo Constitucional de Francia.

Consejo Constitucional de la República francesa, sentencia número 2009/580 DC de 10 junio 2009, [en línea], http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2009580DCes2009_580dc.pdf

3.9. Jurisprudencia administrativa.

Resolución R/01676/2015 de la Agencia Española de Protección de Datos (AEPD), [en línea], http://www.agpd.es/portalwebAGPD/resoluciones/procedimiento_apercibimiento/procedimiento_apercibimiento_2015/common/pdfs/A-00119-2015_Resolucion-de-fecha-01-07-2015_Art-ii-culo-22.2-LSSI.pdf

Resolución R/01116/2015 de la AEPD, [en línea], http://www.agpd.es/portalwebAGPD/resoluciones/procedimiento_apercibimiento/procedimiento_apercibimiento_2015/common/pdfs/A-00055-2015_Resolucion-de-fecha-13-05-2015_Art-ii-culo-6-LOPD.pdf

4. WEBGRAFÍA

Agencia Catalana de Protección de Datos (APDCAT), consultable en: http://www.apd.cat/es

Agencia Española de Protección de Datos, consultable en, https://www.agpd.es/portalweb/index-ides-idphp.php

Agencia Estatal Boletín Oficial del Estado del Ministerio de la Presidencia, consultable en, www.boe.es

Agencia Vasca de Protección de Datos (AVPD), consultable en: http://www.avpd.euskadi.eus/s04-5213/es/

Alfa-Redi (Latinoamérica y el Caribe)

Amnesty International USA

Amnistía Internacional, Campaña dejen de seguirme, [en línea], https://www.amnesty.org/es/get-involved/unfollowme/

Asociación Instituto de Normas Técnicas de Costa Rica (INTECO): http://www.inteco.or.cr/esp/index.html

Asociación para el Progreso de la Comunicaciones: http://derechos.apc.org/charter.shtml

Asociación para el Progreso de las Comunicaciones, consultable en: https://www.apc.org/es/node/93

Big Brother Watch, (Reino Unido).

Centro Europeo de Estudios Nucleares (CERN), http://public.web.cern.ch/public/

Cumbre Mundial sobre la Sociedad de la Información consultable en: http://www.itu.int/wsis/index-es.html

DEA's Office of National Security Intelligence (ONSI), www.dea.gov

Defense Intelligence Agency (DIA), www.dia.mil

DHS Office of Intelligence & Analysis, http://www.dhs.gov/office-intelligence-and-analysis

Electronic Frontier Foundation, consultable en: https://www.eff.org/es

Electronic Privacy Information Center - EPIC (EE.UU.)

Energy Office of Intelligence & Counter-Intelligence, http://energy.gov/office-intelligence-and-counterintelligence

Federal Bureau of Investigation (FBI), www.fbi.gov

Free Network Foundation (EE.UU.)

Gobierno Digital de Costa Rica: http://www.gobiernofacil.go.cr/gobiernodigital/index.html

Human Rights Watch (EE.UU.)

Human Rights Watch, "UK: Human Rights Watch Challenges Surveillance", [en línea], https://www.hrw.org/news/2015/09/14/uk-human-rights-watch-challenges-surveillance

Iniciativa de Accesibilidad Web, conocida como WAI (Web Accessibility Initiative): http://www.w3c.es

Instituto Costarricense de Electricidad: http://www.grupoice.com/

Instituto Federal de Acceso a la Información Pública, México: http://www.ifai.org.mx/

Internet Assigned Numbers Authority (IANA), consultable en: https://www.iana.org/numbers

Internet Society, consultable en: http://www.internetsociety.org/

La Declaración de Principios de Ginebra, de la Cumbre Mundial sobre la Sociedad de la Información se puede consultar en: http://www.itu.int/wsis/documents/doc_multi.asp?lang=es&id=1161|1160

National Geospatial-Intelligence Agency (NGA), www.nga.mil

National Security Agency (NSA), www.nsa.gov

Necessary and Proportionate Principles, “International Principles on the Application of Human Rights to Communications Surveillance”, [en línea], https://es.necessaryandproportionate.org/

Organización de las Naciones Unidas: http://www.un.org/spanish/

Privacy Activism (EE.UU.)

Privacy International, consultable en: https://www.privacyinternational.org/

Programa Nacional para la Sociedad de la Información Argentina: http://www.psi.gov.ar

RACSA (Radiográfica Costarricense S.A.): http://www.racsa.co.cr/index.html

Sitio en español de la Cumbre Mundial sobre la Sociedad de la Información: http://www.itu.int/wsis/index-es.html

State Bureau of Intelligence & Research, http://www.state.gov/s/inr/

Treasury Office of Intelligence & Analysis, http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Intelligence-Analysis.aspx

Unión Internacional de Telecomunicaciones (UIT): http://www.itu.int/wsis/index-es.html

United States Air Force, http://www.airforce.com/

United States Army, http://www.army.mil/

Wikimedia, (EE.UU.).