XIX Edición del Premio Protección de Datos Personales de Investigación
de la Agencia Española de Protección de Datos

PREMIO IBEROAMÉRICA 2015

Hábeas data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001:2013

Luis Fernando Cote Peña

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

BOLETÍN OFICIAL DEL ESTADO
MINISTERIO DE LA PRESIDENCIA

HÁBEAS DATA EN COLOMBIA
UN TRASPLANTE NORMATIVO
PARA LA PROTECCIÓN DE LA DIGNIDAD
Y SU CORRELACIÓN CON LA
NTC/ISO/IEC 27001:2013

HÁBEAS DATA EN COLOMBIA UN TRASPLANTE NORMATIVO PARA LA PROTECCIÓN DE LA DIGNIDAD Y SU CORRELACIÓN CON LA NTC/ISO/IEC 27001:2013

Luis Fernando Cote Peña

Premio Protección de Datos Personales de Investigación 2015 Iberoamérica

Agencia Española de Protección de Datos

Agencia Estatal Boletín Oficial del Estado
Madrid, 2016

NIPO: 007-16-099-5
ISBN: 978-84-340-2313-0

IMPRENTA NACIONAL DE LA AGENCIA ESTATAL
BOLETÍN OFICIAL DEL ESTADO
Avda. de Manoteras, 54. Madrid 28050

A Erika, mi fortaleza, y a mis hijos
Luis Fernando y Sara Teresa, mi motivación.

Índice

Prólogo 14

1. Introducción 16

2. Principio de dignidad humana y Hábeas Data

2.1 El problema conceptual 21
2.2 Dimensionamiento de la dignidad 24
2.2.1 La noción restrictiva de dignidad 24
2.2.2 La noción universal de dignidad 30
2.3 Dignidad como derecho subjetivo y soporte del Hábeas Data 40
2.3.1 La dimensión activa de la dignidad 41
2.3.2 La dimensión pasiva de la dignidad 44
2.4 Núcleo de la Dignidad 45
2.5 Las singularidades del ser humano nexo entre Dignidad y Hábeas Data 47

3. Del núcleo a la periferia, el trasplante normativo de la protección de datos

3.1 Antecedentes históricos 51
3.2 La diáspora jurídica 56
3.2.1 Periodo pre-dignidad 56
3.2.2 Periodo de fundamentación humanista 57
3.2.3 Periodo de insularidad normativa 60
3.2.4 Periodo de unificación europea 63
3.2.5 Periodo de trasplante normativo 67

4. Hábeas Data en Colombia

4.1 Marco socio político de surgimiento del Hábeas Data 72
4.2 Marco regulatorio colombiano del Hábeas Data 75
4.2.1 Reglamentación jurisprudencial del Hábeas Data. El camino hasta la autonomía 76
4.2.2 Reglamentación del Hábeas Data Financiero (Ley 1266 de 2008) 81
4.2.3 Reglamentación del Hábeas Data Penal (Ley 1273 de 2009) 82
4.2.4 Reglamentación del Hábeas Data de personas naturales (Ley 1581 de 2012) 88
4.3 Principios rectores del Hábeas Data 89
4.3.1 Principio de Dignidad (PC) 90
4.3.2 Principio de Legalidad (PL) 90

4.3.3 Principio de libertad (PL) 90
4.3.4 Principio de veracidad o calidad (PL) 91
4.3.5 Principio de integridad (PL) 91
4.3.6 Principio de finalidad (PL) 92
4.3.7 Principio de acceso y circulación restringida (PL) 92
4.3.8 Principio de transparencia (PL) 93
4.3.9 Principio de seguridad (PL) 93
4.3.10 Principio de confidencialidad (PL) 93
4.3.11 Principio de responsabilidad demostrada (PL) 93
4.3.12 Principio de temporalidad de la información (PL) 94
4.3.13 Principio de interpretación integral de derechos constitucionales (PL) 94
4.3.14 Principio de necesidad (PJ) 94
4.3.15 Principio de utilidad (PJ) 95
4.3.16 Principio de incorporación (PJ) 95
4.3.17 Principio de caducidad (PJ) 96
4.3.18 Principio de individualidad (PJ) 96

4.4 Elementos integradores del Hábeas Data 96

4.4.1 Núcleo esencial y contenido adyacente del derecho fundamental de Hábeas Data en la Ley 1581 de 2012 97
4.4.2 El Dato como objeto de protección del derecho fundamental al Hábeas Data 100
4.4.3 El titular del derecho de Hábeas Data y sus facultades 124
4.4.4 Contrato de Hábeas Data 132
4.4.5 Responsables, encargados y subencargados 140
4.4.6 Autoridades de los datos personales y facultad sancionatoria 146
4.4.7 Transferencia de datos y países seguros 150
4.4.8 Caducidad del dato 158
4.4.9 Conservación del dato 164

5. La ISO/IEC 27001 en Colombia

5.1 Marco histórico socio económico de surgimiento 169
5.2 Marco regulatorio de la norma ISO/IEC 27001-2013 179
5.3 Razones de escogencia de la NTC/ISO/IEC 27001:2013 185

5.3.1 Aceptabilidad internacional 186
5.3.2 Certificabilidad de la norma 187
5.3.3 Robustez del ámbito normativo 187
5.3.4 Referencia institucional para SGSI 188
5.3.5 Referencia normativa para SGSI 189
5.3.6 Obligatoriedad normativa 189
5.3.7 Condición de norma técnica colombiana - NTC - 190

5.4 Principios rectores de la NTC/ISO/IEC 27001 192

5.4.1 Principio de concienciación 192
5.4.2 Principio de responsabilidad 192
5.4.3 Principio de respuesta 192
5.4.4 Principio de valoración de riesgos 192

5.4.5 Principio de diseño e implementación de la seguridad... 193
5.4.6 Principio de gestión de seguridad... 193
5.4.7 Principio de reevaluación... 193

5.5 Elementos integradores de la NTC/ISO/IEC 27001... 194

5.5.1 Núcleo esencial de protección de la norma NTC/ISO/IEC 27001... 194
5.5.2 La información como objeto de protección de la NTC/ISO/IEC 27001... 195
5.5.3 Clasificación de la información... 196
5.5.4 Propietario y responsable de la información... 197
5.5.5 Otros elementos integradores... 198

6. Elementos convergentes y divergentes entre la LEPD y la NTC/ISO/IEC 27001

6.1 Elementos convergentes... 200

6.1.1 Ámbito de acción u operatividad... 200
6.1.2 Gestión sistémica de la seguridad... 201
6.1.3 Exposición de los objetos protegidos a riesgos comunes... 202
6.1.4 Fundamentación en principios... 203
6.1.5 Requerimiento de política... 204
6.1.6 Actores responsables... 205
6.1.7 Gestión de incidentes... 206
6.1.8 Documentación común... 207
6.1.9 Autoridades normativas... 211
6.1.10 Mecanismos de seguridad según caracterización del objeto reglado... 212
6.1.11 Mantenimiento del sistema... 213

6.2 Elementos divergentes... 213

6.2.1 Valoración del objeto de aseguramiento... 214
6.2.2 Obligatoriedad de la norma... 215
6.2.3 Principios diferenciadores... 215
6.2.4 Documentación diferenciada... 215
6.2.5 Exigibilidad de registro externo... 216

7. Conclusiones... 217

8. Referencias... 220

9. Siglas... 231

Lista de figuras

Figura 1.	Relación jurídica del derecho de dignidad	41
Figura 2.	Dimensión normativa de la dignidad	46
Figura 3.	Singularidades protegidas por el Hábeas Data	48
Figura 4.	Registros asociados con el holocausto provocado por el gobierno nazi	52
Figura 5.	Imágenes de la masacre de Badajoz, España, bajo el régimen de Francisco Franco, 1936	53
Figura 6.	Declaración Americana de Independencia de 1776.	57
Figura 7.	La Presidenta de la Comisión de Derechos Humanos, señora Eleanor Roosevelt	58
Figura 8.	Ámbito de regulación de la Ley 1266 de 2008	82
Figura 9.	Ámbito de regulación de la Ley 1581 de 2012	88
Figura 10.	Dimensiones del derecho subjetivo del Hábeas Data. Núcleo Esencial: autodeterminación informática	98
Figura 11.	Relacionamiento dato-información	102
Figura 12.	Datos públicos	114
Figura 13.	Datos personales de riesgo alto	115
Figura 14.	Datos personales de riesgo medio	116
Figura 15.	Datos privados de riesgo bajo	119
Figura 16.	Parámetros de *accountability* o responsabilidad demostrada.	145
Figura 17.	Criterios de graduación de sanciones	147
Figura 18.	Estonia 2007 – Caso documentado más grande de la historia de un ciberataque	172
Figura 19.	Registro de ataques de ciberseguridad y respuestas gubernamentales	173
Figura 20.	Registro de noticias de la Fiscalía General de la Nación sobre delitos informáticos	174
Figura 21.	Modelo de coordinación	175
Figura 22.	Relación entre seguridad de la información y ciberseguridad	178
Figura 23.	Propósito normativo de la LEPD y la NTC/ISO/IEC 27001:2013	201
Figura 24.	Imagen de correlación de los SGSI y SGSDP	218

Lista de tablas

Tabla 1.	Reglas de caracterización de la información y de los datos.	104
Tabla 2.	Cesión-comunicación y transmisión de datos.....	149
Tabla 3.	Comparativo de la LOPD y la LEPD sobre transmisión de datos.....	150
Tabla 4.	Eventos de intercambio internacional de datos regulados...	153
Tabla 5.	Eventos de intercambio internacional de datos no regulados.	154

Glosario

Amenaza: Factores internos o externos que pueden tomar ventaja de una vulnerabilidad y generar de ésta manera un riesgo.

Bases documentales – BD: Corresponde al conjunto de documentos jurídicos o de soporte del tratamiento de Datos Personales que relacionan el Talento Humano – TH, usuarios, clientes y/o terceros, con la Organización. Vr. gr. contratos, reglamentos, protocolos, convenios, etc.

Ciclo R. A. U. C. S.: Constituye el ciclo de vida de los datos personales al interior de una organización, y hace referencia a las operaciones que se efectúan sobre los mismos, esto es: recolección, almacenamiento, uso, circulación y supresión.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Diáspora jurídica: Fenómeno de expansión de marcos normativos desarrollados en el núcleo del conocimiento pare ser replicados en la periferia.

Dignidad: Valor, principio o regla superior de un ordenamiento jurídico. También se entiende como condición universalmente reconocida a todos los seres humanos.

Encargado del tratamiento: Conforme a la ley, es la persona natural o jurídica, pública o privada, que por cuenta de un Responsable trata datos personales.

Fuente de información: Conforme a la ley, es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final.

Gestión del riesgo: Hace referencia a las medidas adecuadas y efectivas que permiten dar solución a los riesgos relacionados con el tratamiento de datos personales.

Hábeas data: Derecho fundamental que otorga a su titular autodeterminación informática y exigibilidad de aseguramiento de sus datos cuando un tercero los trata.

Infraestructura de Tecnologías de la Información y las comunicaciones – TIC: Corresponde a los elementos tecnológicos informáticos (software, hardware, redes, formatos de captura, archivos, archivadores, etc.) o de cualquier otra naturaleza que se utilizan para tratar datos personales.

Locaciones físicas: Se tiene por locaciones físicas de información, los archivadores de información físicos con que cuenta la organización, en los cuales existe alojamiento de datos personales de los diferentes titulares.

Marco regulatorio: Conjunto de normas jurídicas referidas a un determinado instituto jurídico.

Núcleo: Centro geográfico de producción de conocimiento normalmente ubicado en los países desarrollados.

Operador de información: Conforme a la ley, se denomina operador de información a la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley.

Organización: Corresponde a la institución (pública o privada) que es objeto de intervención por el equipo asesor.

Periferia: Lugar geográfico distante de los núcleos de generación de conocimiento, generalmente ubicado en países en vías de desarrollo.

Responsable del tratamiento: Conforme a la ley, es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otro, decide sobre la base de datos y/o el tratamiento de los datos.

Riesgo: Acontecimiento probable que una amenaza puede llevar a cabo valiéndose de una vulnerabilidad, generando un impacto negativo sobre la información.

Singularidades: conjunto de datos personales asociados a un individuo de la especie humana, que en su conjunto le hacen diferente de los demás.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP): Sistema de gestión para la implementación, conservación, modificación, actualización y el mejoramiento del tratamiento y seguridad de los datos personales, en conformidad con la Ley de un país.

Subencargado del tratamiento: Conforme a la ley, es la persona natural o jurídica, pública o privada, que por cuenta de un encargado, trata datos personales.

Talento humano – TH: Corresponde a las personas que, dentro de la organización, desarrolla actividades vinculadas al tratamiento de datos personales.

Titular del dato: Se entiende por titular del dato al universo de individuos a quienes corresponde los datos cuya protección se pretende.

Tratamiento del dato: Conforme a la ley, cualquier operación o conjunto de operaciones sobre datos personales que conforman el ciclo R. A. U. C. S.

Trasplante normativo: Proceso de incorporación a un ámbito jurídico nacional de un cuerpo normativo proveniente de un sistema jurídico extranjero.

Vulnerabilidad: Es la debilidad o carencia de la capacidad y condiciones para responder ante una amenaza que puede generar un riesgo.

Resumen

La globalización impactó a América Latina finalizando el siglo xx, motivando los gobiernos a realizar ajustes en sus constituciones, modificar las legislaciones y buscar nuevos horizontes económicos. En Colombia, el primer paso fue el ajuste constitucional de 1991 que incorporó la dignidad como principio superior y, con él, un catálogo adicional de derechos fundamentales, entre otros el de Hábeas Data. Luego, vinieron desarrollos legislativos que, en seguimiento a orientaciones de la OCDE y acatamiento a llamados de la Corte Constitucional, permitieron la aparición de la ley 1266 de 2008 de Hábeas Data financiero y, posteriormente, la ley 1581 de 2012 y sus Decretos 1377 de 2013 y 886 de 2014 de protección de los datos personales.

El nuevo universo jurídico asociado al Hábeas Data estableció una serie de obligaciones a entidades públicas y privadas que tratasen datos personales en sus operaciones, pero, no obstante los desarrollos jurisprudenciales, legislativos, reglamentarios y doctrinales, en Colombia aún no se logra definir claramente el alcance de las nuevas exigencias legales.

Con el propósito de buscar líneas de orientación para la definición de los mencionados alcances obligacionales, se propuso un análisis de elementos convergentes y divergentes entre la ley 1581 de 2012 y la NTC/ISO/IEC 27001:2013, en el entendido de considerar esta última, el estándar internacional más adecuado para la gestión de la seguridad de la información, universo al cual pertenecen los datos personales. Para el logro del cometido, se abordó el desarrollo del Hábeas Data desde la perspectiva de la dignidad, para, posteriormente efectuar un recorrido descriptivo del estándar internacional, presentándose en la fase final los resultados del cotejo normativo y las conclusiones que de ello se derivaron.

De esta manera se deja presentado este trabajo como contribución a la larga tarea pendiente por buscar la decantación doctrinal del nuevo instituto jurídico del Hábeas Data.

Palabras claves: Dignidad, Hábeas Data, ISO 27001, Protección de Datos Personales, Seguridad de la Información.

Abstract

Globalization impacted Latin America by the end of the Twentieth century, motivating governments to perform adjustments on its constitutions, modify laws and look for new economic horizons. In Colombia, the first step was the constitutional adjustment of 1991, which introduced dignity as a higher principle, and with it, an additional catalog of fundamental rights, having Habeas Data amongst them. Afterwards, several legislative developments came about, by following OCDE orientations and adhering to the appeals from the Constitutional Court, which allowed the emergence of law 1266 about Financial Habeas Data in 2008 and later the law 1581 about Personal Data Protection in 2012, along with its decrees 1377 and 886 in 2013 and 2014 respectively.

The new legal universe associated to Habeas Data, established a set of obligations for public and private entities which provided treatment of personal data in its operations, but, in spite of the jurisprudential, legislative, regulative and doctrinal developments, it is not possible to define clearly the scope of the new legal requirements in Colombia.

With the purpose of seeking orientation guidelines for the definition of the aforementioned obligatory scope, a divergent and convergent analysis is proposed, between law 1581 (2012) and the NTC/ISO/IEC 27001:2013 framework, on the understanding of considering the second, the most suited international standard for Information Security Management, which is a universe where personal data belong. To achieve this goal, the Habeas Data has been approached from the perspective of dignity, in order to make a descriptive route of the international standard, presenting in the final phase, the results of the normative checking and the conclusions derived from this study.

In this manner, this work is presented as a contribution to the long and continuous task of searching the doctrinal decantation of the new legal institute of Habeas Data.

Keywords: Dignity, Habeas Data, ISO 27001, Personal Data Protection, Information Security.

Prólogo

La Agencia Española de Protección de Datos convoca anualmente el Premio de Protección de Datos Personales de Investigación con el objetivo de fomentar y promocionar los trabajos más destacados en esta materia. En su edición XIX el Jurado ha otorgado el accésit al trabajo *Big data, privacidad y protección de datos*, de Elena Gil González, una obra que analiza el impacto en el derecho a la privacidad de este nuevo fenómeno que implica el tratamiento y almacenamiento masivo de información.

Uno de los retos actuales de la Agencia, tal y como se recoge en su Plan Estratégico 2015-2019, es que la innovación y la protección de datos discurran de forma paralela. La protección de datos es un factor crítico para conseguir un correcto afianzamiento de la sociedad de la información, determinante para proporcionar productos y servicios respetuosos y de calidad, y, especialmente, para generar confianza en los usuarios de los mismos. La Agencia quiere contribuir a que el sector empresarial consiga un elevado cumplimiento de las obligaciones que la normativa de protección de datos les impone, fomentando una cultura de la protección de datos que suponga una clara mejora de la competitividad, compatible con el desarrollo económico. Para ello, es necesario apostar por políticas proactivas de cumplimiento que permitan detectar el impacto que los nuevos desarrollos tecnológicos pueden tener en la privacidad de los ciudadanos, buscando mitigar los riesgos sin que, en ningún caso, haya que renunciar a las funcionalidades y beneficios que estos proporcionan.

En este sentido, el Big Data es un reflejo del paradigma actual de la sociedad de la información y del impacto de la tecnología en la esfera de la vida privada. El despliegue de tecnologías como el big data, el internet de las cosas, el uso de wearables o las smartcities, entre otras, requiere de un análisis y valoración técnica y jurídica para promover buenas prácticas que garanticen su adecuación a la normativa de protección de datos y, en consecuencia, el respeto por los derechos de los ciudadanos.

El trabajo de investigación que el lector encontrará a continuación aborda el big data desde una perspectiva optimista, buscando el acer-

camiento entre los beneficios sociales y económicos que puede aportar sin soslayar la garantía del derecho a la protección de datos de las personas.

La obra contribuye a difundir algunos aspectos esenciales de esta tecnología, aportando propuestas para minimizar los riesgos de intrusión en la privacidad. El deber de transparencia y consentimiento, las técnicas de anonimización, la privacidad por defecto y desde el diseño que se abordan en el trabajo son elementos esenciales para un desarrollo respetuoso del big data.

Mar España Martí
Directora de la Agencia Española de Protección de Datos

1. INTRODUCCIÓN

El proceso de globalización que impactó a América Latina durante la última década del siglo xx motivó a los gobiernos del área a realizar ajustes estructurales en sus constituciones, modificar sus legislaciones y lanzarse en la búsqueda de nuevos horizontes económicos. En desarrollo de tales circunstancias se celebraron acuerdos de libre comercio con países de otras latitudes y establecieron relacionamientos con organismos internacionales que, creados por estos, buscan la estandarización de principios y normativas así como la incorporación cultural de buenas prácticas en diversos aspectos de la vida empresarial y gubernamental, necesarios para facilitar los intercambios transfronterizos.

Este ha sido el caso por ejemplo de la Organización para la Cooperación y el Desarrollo Económico –OCDE–, entidad que hoy agrupa cerca de 34 Estados, entre ellos Estados Unidos, Reino Unido, Francia, Alemania, Japón, España, en Latinoamérica Chile y México, y al cual aspira Colombia ingresar en el año 2016. En el caso colombiano, como en los demás países de la zona, para lograr su ingreso, se han impuesto trasplantes normativos en diferentes áreas, como por ejemplo contables (Normas Internacionales de Información Financiera –NIIF– y Normas Internacionales de Contabilidad para el Sector Público –NICSP–), de protección al consumidor y, para el caso que nos interesa, normas de protección de datos personales o Hábeas Data.

El primer paso se dio en Colombia con el ajuste de la Constitución Política en el año 1991, en el cual, entre otros muchos asuntos, se incorporó la dignidad como principio superior y con él un catálogo adicional de derechos fundamentales como el buen nombre, la intimidad y el propio Hábeas Data. Este último se incorporó en el artículo 15, señalando que todas las personas «… tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas…», advirtiendo que en «… la recolección, tratamiento y circulación de datos» se deben respetar «… la libertad y demás garantías consagradas en la Constitución».

Con posterioridad, siguiendo las orientaciones de la OCDE y en acatamiento a pronunciamientos de la Corte Constitucional, en desarrollo del mandato superior, el Congreso de Colombia expidió la Ley 1266 de 2008 por medio de la cual se reglamentó el Hábeas Data para las personas naturales y jurídicas en relación con los datos referidos a asuntos económicos y financieros, y posteriormente, la Ley 1581 de 2012 y sus Decretos 1377 de 2013 y 886 de 2014 que concretaron el marco regulatorio de la protección de los datos personales, estos dos últimos decretos ahora incorporados literalmente en el Decreto 1074 del 26 de mayo de 2015 o Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sumado a la Circular Externa No. 2 del 3 de Diciembre de 2015 sobre registro nacional de bases de datos o RNBD.

De esta forma se fue dando el trasplante normativo que, por una parte, otorgó a las personas la facultad de la autodeterminación informática y exigibilidad de protección de datos personales, conjunto de derechos aún muchos de ellos desconocidos por sus titulares y, por la otra, impuso a las organizaciones públicas y privadas que tratan datos personales, obligaciones que demandan la incorporación de ajustes en sus operaciones internas y externas, a fin de lograr su conformidad con la ley y evitar los riesgos jurídicos por inadecuado tratamiento de datos, pudiéndose traducir en demandas de responsabilidad civil, imputaciones penales, sanciones administrativas por parte de la Superintendencia de Industria y Comercio y, en algunos casos, incluso juicios de responsabilidad fiscal y disciplinaria.

No obstante, los desarrollos jurisprudenciales, legislativos, reglamentarios y doctrinales en Colombia, a la fecha no han definido claramente el alcance de las obligaciones impuestas a las entidades que tratan los datos personales para lograr la conformidad, resultando necesario buscar, para el caso nacional, herramientas que direccionen la definición de los marcos en que han de moverse los responsables y encargados, no solo para proteger a los titulares de los datos que tratan, sino también para efectos de evitar los riesgos jurídicos que el indebido tratamiento les puede derivar a aquellos.

En tal sentido, se consideró como hipótesis que, entre la Ley 1581 de 2012 y los estándares internacionales que se han desarrollado para la gestión de los riesgos asociados a la seguridad de la información y en particular la NTC/ISO/IEC 27001:2013, identificada como la más

adecuada por las razones que en el desarrollo del trabajo quedaron expresadas; existían elementos convergentes, no obstante los divergentes, que podrían servir como insumo para la demarcación de las acciones apropiadas y efectivas que debían asumirse por responsables y encargados, es decir, el marco referenciador de sus respectivas obligaciones.

A efectos de demostrar la hipótesis argumentada, se propuso metodológicamente en primer lugar, desarrollar un ejercicio analítico descriptivo de la protección de datos personales desde la perspectiva de la dignidad a partir de las normas colombianas y en especial la Ley 1581 de 2012. En un segundo lugar, proceder en igual sentido a realizar un análisis descriptivo de la norma NTC/ISO/IEC 27001/2013, para posteriormente, mediante la metodología analítico-reflexiva, contrastar, entre otros aspectos, las cargas impuestas por la ley a las organizaciones que tratan datos personales en sus operaciones, con los elementos relevantes de los sistemas de gestión de la seguridad de la información reglados por la norma NTC/ISO/IEC 27001:2013.

El resultado de la labor investigativa se presenta descrita capitularmente de la siguiente manera: en el primer capítulo se describe la Dignidad como el valor superior que regla todo el universo del Hábeas Data. Para el efecto se define, entre las líneas conceptuales de Dignidad Restringida y Dignidad Universal, aquella que se ha adoptado para explicar el surgimiento del Hábeas Data y a partir de la cual, soportados en los conceptos de Igualdad y Libertad, se explica la relación entre el núcleo esencial de la Dignidad y las singularidades de los sujetos, esto es los datos personales que constituyen el objeto material de protección del Hábeas Data. En un segundo capítulo se ponen de presente los antecedentes históricos y jurídicos del instituto del Hábeas Data y su relación con el concepto de Dignidad Universal, a partir de los cuales se evidencia que la normativa colombiana ha sido un trasplante jurídico europeo altamente inducido por los fenómenos de globalización y por sobre todo de la influencia de la Organización para la Cooperación y el Desarrollo Económico –OCDE–. Adicionalmente, en el tercer capítulo, al inicio se realiza la descripción analítica del Hábeas Data en función de la Ley 1581 de 2012, para lo cual se describe el marco político de surgimiento, se identifica el desarrollo jurisprudencial nacional y se refieren otros marcos normativos asociados como la Ley 1266 de 2008 de datos financieros y la Ley 1273 de 2009 sobre tipos penales relacionados con la informa-

ción y los datos. En un segundo momento de este capítulo, se describen los principios legales y jurisprudenciales que rigen el Hábeas Data, para finalmente referir los elementos que conforman el universo del nuevo instituto, tales como el núcleo esencial del derecho, el dato como objeto material del mismo, el titular de los datos y el negocio jurídico denominado contrato de Hábeas Data, los responsables, encargados y subencargados, el ámbito de operatividad de los datos personales, las autoridades de los datos personales y la transferencia de los mismos. Durante todo el recorrido descriptivo que se realiza del instituto, se hace referencia a fuentes europeas que refuerzan la condición del trasplante normativo y explican las dificultades que de ello se derivan al momento de su aplicación en el ámbito jurídico nacional. Un cuarto capítulo se destina a la descripción analítica de la norma NTC/ISO/IEC en Colombia, obviamente referenciando en un primer momento los aspectos históricos del surgimiento de la norma, luego los marcos regulatorios asociados a la misma, para luego explicar las razones que se tuvieron para escoger esta y no otra norma de los múltiples estándares internacionales que en materia de seguridad de la información existen. Después de abordar tales temas, se procedió a identificar los principios rectores de la norma, sus elementos integradores, entre otros su núcleo esencial, la información como objeto de protección y su clasificación, además de los sujetos relacionados con ella, es decir, los propietarios y responsables de la misma. El quinto capítulo, por su parte, inicia describiendo los elementos convergentes entre la LEPD y la NTC/ISO/IEC 27001:2013, desde la perspectiva del ámbito de acción u operatividad, la gestión sistémica de la seguridad, la exposición al riesgo de los objetos protegidos, los principios en los que se fundamentan las normas, la exigibilidad de la política, los actores vinculados, las acciones para la gestión de incidentes, la obligación de documentar, las autoridades que regulan cada uno de los universos, los mecanismos de aseguramiento y mantenimiento de los sistemas de gestión de los objetos de cada uno de las normas analizadas. Y, finaliza este capítulo con los elementos divergentes expuestos en función de los conceptos de valoración del objeto protegido por las normas, la obligatoriedad o no de las mismas, los principios diferenciadores, las particularidades documentales para el *accountability* y las obligaciones de registros externos. Finalmente, en el sexto capítulo se presentan las conclusiones con base en las cuales ha quedado demostrada la hipótesis planteada sobre la existencia de

los elementos convergentes y divergentes de los dos mundos analizados, esto es el de la NTC/ISO/IEC 27001:2013 y el de la LEPD de Colombia. Pero, quizá la mayor importancia de las conclusiones extraídas es el reconocimiento de la falta de claridad jurídica respecto de las obligaciones concretas de las organizaciones que tratan datos personales, para tener la confianza legítima de saberse cumpliendo las exigencias de la LEPD, confianza que se puede alcanzar de mejor forma si se desarrolla un *framework* certificable, conforme al sistema nacional de acreditación colombiano, para lo cual, la NTC/ISO/IEC 27001:2013, y los resultados de esta investigación, pueden constituir base para tal propósito.

2. PRINCIPIO DE DIGNIDAD HUMANA Y HÁBEAS DATA

2.1 EL PROBLEMA CONCEPTUAL

Permanentemente se lee y oye referir acerca de la *dignidad* en espacios cotidianos, políticos o académicos, haciendo referencia a aspectos diversos y muchas veces difícilmente inteligibles. Un ejemplo referencia a la dignidad por parte de un actor político, lo constituye el discurso del presidente de los Estados Unidos, Barack Obama (Obama, 2013) refiriéndose a Nelson Mandela, cuando utiliza la palabra dignidad como sinónimo de talante, al afirmar: «Su dignidad y su esperanza se hacía sentir en su vida». Así mismo, Nelson Mandela, citado por el mismo presidente Obama, refería a la indignidad como las condiciones que degradan la existencia humana así: «la ira nace de mil desaires, mil indignidades, mil momentos no recordados... el deseo de luchar contra el sistema que aprisionaba mi gente» (ibídem). Esta circunstancia se hace aún más palmaria en los ambientes jurídicos, donde su precisión conceptual cobra vital importancia, como por ejemplo cuando se aborda el tema de los derechos fundamentales y en especial el derecho de Hábeas Data, el cual se refiere permanentemente muy ligado a la Dignidad Humana.

De hecho, hoy en día se ha vuelto común la referencia a la Dignidad en casi todos los textos constitucionales de las naciones que se denominan democráticas, muchas de ellas incorporando concomitantemente el derecho a la protección de los datos personales. Sirve de ejemplo de lo afirmado las siguientes referencias a países en cuya constitución la Dignidad está claramente reconocida como valor superior:

España, por ejemplo en el artículo 10.1 de la Constitución Política de 1978 define que «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».

La Ley Fundamental para la República Federal Alemana de 1949, (modificado 31/08/1990) en su artículo 1.1. señala que «La dignidad

del hombre es sagrada y constituye deber de todas las autoridades del Estado su respeto y protección».

En Italia, la Constitución de 1947 en el artículo 3o advirtió que «Todos los ciudadanos tendrán la misma dignidad social y serán iguales ante la ley, sin distinción de sexo, raza, lengua, religión, opiniones políticas ni circunstancias personales y sociales».

En China, su Constitución de 1982 ha establecido en su artículo 38.º que «La dignidad personal de los ciudadanos de la República Popular China es inviolable. Se prohíbe ofenderlos, denigrarlos o lanzarles acusaciones infundadas e imputaciones insidiosas por cualquier medio».

México, en su carta superior de 1917 con su reforma del año 2011, en el inciso 5.º de su artículo 1.º, ha establecido que «Queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas», en concordancia con los artículos 2.º, 3.º y 25.º

Pareciera, por su uso frecuente, que pretender aclarar su dimensión constituye esfuerzo sin sentido, el que podría tornarse aún más superfluo si se trata de discutir su aceptación o no, como atributo o cualidad propia del ser humano. No obstante, muchas realidades ocurren frente a nuestros ojos y sobre las cuales podríamos consensuar que evidencian hechos que denominaríamos indignos sin duda alguna, tal como ocurre con la xenofobia, el racismo, la segregación por razones de salud, la mendicidad de ancianos y de niños, el reclutamiento forzado de menores, las hambrunas masivas, la discriminación de la mujer, las desapariciones forzadas, el bombardeo de poblaciones civiles, la explotación de menores, la trata de personas, etc. En muchos de estos ignominiosos comportamientos, la utilización de los datos personales constituye elemento que facilita tan reprochables actos.

Por tal razón, ante este contraste que se da entre los consensos lingüísticos sobre el reconocimiento de la Dignidad y aquellas realidades inaceptables que exacerban el alma, oportuno se torna volver a esta temática, para realizar este primer esfuerzo de definición conceptual que se demanda entonces, para precisar el ámbito conceptual,

identificar la actualidad y trascendencia, y por su puesto definir la dimensión que desde la esfera jurídica se dará a la Dignidad, determinando a partir de ello el nexo vinculante que hay entre este renovado valor jurídico y el recientemente aparecido instituto de la protección de datos personales.

En tal propósito, resulta necesario iniciar acotando que la palabra Dignidad proviene del latín *dignitâs, dignitâtis:* «dignidad», referida a una expresión romana que reconoce una determinada condición social. Este origen se encuentra manifiesto en todas las acepciones que del vocablo *dignidad* trae el Diccionario de Lengua Española [Real Academia Española, Diccionario de la Lengua Española (DRAE), 2012] así:

1. f. Cualidad de digno.
2. f. Excelencia, realce.
3. f. Gravedad y decoro de las personas en la manera de comportarse.
4. f. Cargo o empleo honorífico y de autoridad.
5. f. En las catedrales y colegiatas, prebenda que corresponde a un oficio honorífico y preeminente, como el deanato, el arcedianato, etc.
6. f. Persona que posee una de estas prebendas. U. t. c. m.
7. f. Prebenda del arzobispo u obispo. Las rentas de la dignidad.
8. f. En las órdenes militares de caballería, cargo de maestre, trece, comendador mayor, clavero, etc.

Es decir que, gramaticalmente hablando, el término hace referencia más a la condición de un determinado individuo de la raza humana en razón de un estatus de privilegio (por su cargo, oficio desempeñado o reconocimiento por parte de alguien en particular, por ejemplo un agente de la iglesia o las instituciones armadas) que a una condición natural del ser humano y por tanto susceptible de pregonarse de todos los miembros de la especie, en otras palabras el lenguaje español le da a la palabra dignidad un sentido eminentemente restrictivo.

No obstante la dimensión semántica originaria de la palabra Dignidad, que lingüísticamente pareciera conservarse desde la perspectiva diacrónica del lenguaje, se han evidenciado manifestaciones conceptuales diversas en el universo del derecho, hábitat natural del lenguaje que lo es, con implicaciones jurídicas variadas y profundas.

Esto explica, para los fines de este trabajo, la necesidad de aproximarse a las dimensiones que la palabra dignidad ha tenido durante algunos momentos de la historia, muchas veces con alcances incluso contradictorios. De esta manera se busca definir una línea conceptual base en que se apoyarán la conclusiones preliminares del trabajo, identificando cuál de las varias concepciones que sobre dignidad se han dado, sea la adoptada para abordar la investigación que se propone en materia de protección de datos personales.

2.2 DIMENSIONAMIENTO DE LA DIGNIDAD

Dos grandes dimensiones pueden recoger la multiplicidad de interpretaciones filosóficas que al término dignidad se le ha dado a través de la historia. Por una parte la que se podría denominar noción restrictiva de la dignidad que parte de considerar la dignidad como un atributo particular de ciertos y determinados miembros de un grupo social en un contexto espacio-temporal definido, a partir del cual sus titulares asumen por tanto una cierta condición de élites. Por la otra, la noción universal de dignidad (a la que en adelante se referirá cada vez que se mencione la palabra dignidad, salvo que se realice advertencia en contrario) que expresa la idea del reconocimiento generalizado de tal cualidad a todos y cada uno de los miembros de la especie humana. Estas dos contrapuestas posiciones han tenido diferentes matices según el momento histórico o la condición del pensador que las hubiere abordado, razón por la cual resulta de importancia hacer una breve referencia a algunas de ellas.

2.2.1 LA NOCIÓN RESTRICTIVA DE DIGNIDAD

Que parte de reconocer la existencia de diferencias esenciales entre los seres humanos, constituye explicación y por tanto justificación de condiciones de desigualdad jurídica. Son ejemplo claro de estas nociones las que marcaron el pensamiento de las culturas antiguas, donde la calidad de digno estaba íntimamente relacionada con reconocimientos personales logrados por los individuos, su condición de ciudadano de un determinado Estado o por el ejercicio de cargos políticos o militares. Tales criterios servían de base para llegar a argumentar que el atributo de la dignidad estaba dado por razón de la

naturaleza misma que, se entendía, hacía diferentes a los seres humanos desde el momento mismo de nacer.

Aristóteles (Aristóteles, 2005, pp. 102, 104, 105) por ejemplo, justificando la esclavitud, afirmaba:

> «La vida es acción, no producción y por ello, el esclavo es un subordinado para la acción… Aquellos hombres que se diferencian de los demás tanto como el alma de cuerpo o como el hombre de la bestia (se hallan en esta condición aquellos cuya función se limita al uso de su cuerpo y eso es lo mejor que tienen), son esclavos por naturaleza… Es por tanto evidente que por naturaleza unos son libres y otros esclavos, y que para éstos últimos es conveniente y justo poseer tal condición.»

Este evidente determinismo que marcó muchos siglos hasta muy entrado el medioevo, resulta inaceptable, a más de absolutamente reprochable, pues al rompe agrede la lógica actualmente imperante en el mundo democrático.

Por otra parte, dentro de estas vertientes antiguas, algunas que se rehusaron al determinismo natural aristotélico, basaban la calidad de digno solo en función de las condiciones intelectuales o cognitivas de las personas. Así, por ejemplo quien, lo expresaba Platón, que en palabras de Antonio Pelé (Pelé, 2010, p. 94).

> «No definía el valor del ser humano en función de su cargo político, del reconocimiento social o de sus honores. El valor del Hombre venía de su única y propia virtud. El decoro externo o el rango político, no eran los elementos constitutivos de la dignidad del Hombre. Esta derivaba solo de su intelecto y de su capacidad para adecuar su conducta con las normas morales.»

Hay que reconocer que sin lugar a dudas este planteamiento platónico constituye una visión un tanto más humanista que la aristotélica, en cuanto que al concebir la posibilidad de adquirir la calidad de dignidad si con antelación se estuviere privado de ella, a partir del acceso al conocimiento y alcance de la sabiduría, salva la condena natural que el aristotelismo imponía. Sin embargo, la dignidad, en términos platónicos, no obstante sus iniciales luces de humanismo, plausibles sin lugar a dudas para la época, visto a la luz de las circunstancias modernas, llevaría a la condena de indignidad de quienes, por las inequidades sociales, no han tenido acceso a los espacios privilegiados del conocimiento. Tal planteamiento resulta por tanto tan reprochable como el aristotélico mismo.

Estos planteamientos de dignidad restrictiva antes enunciados, podrían pensarse cosa del pasado antiguo. Sin embargo, tal percepción para nada corresponde a la realidad. Esta línea del pensamiento, mantuvo vigencia durante casi medio siglo xx a través de las corrientes ideológicas que alimentaron el pensamiento político nacionalista como el nazi o el fascista. La defensa de este pensamiento, alimentado en las canteras ideológicas de filósofos como Carl Schmitt, como resulta entendible, motiva permanentemente escenarios de discusión política, filosófica y jurídica para nada pacífica. El debate rompe las barreras de la mera discusión filosófica para materializarse en el campo del Derecho donde, con base en dichos planteamientos, se construye la justificación de la inexistencia de principios y valores superiores como la Dignidad y por tanto la igualdad, llegándose a la conclusión de considerar la imposibilidad de la existencia de normas supranacionales a las cuales someter los ordenamientos legales que en cada Estado se desarrollen.

En esta línea ius-filosófica cabe traer a mención nuevamente a Carl Schmitt, para quien las nociones de dignidad son atributo del amigo y por su puesto para nada reconocibles al enemigo sustancial (judíos) (Delgado Parra, 2001). Por ello, y como razón de Estado, las normas jurídicas deberán interpretar y garantizar la existencia del amigo (la raza aria) y a su vez amparar los instrumentos que garanticen la extinción hasta la muerte del enemigo mismo. Schmitt, referido por Gregorio Saravia (Saravia, 2012, p. 157), reforzando lo advertido, señala:

> «La idea de la raza es la gran aportación que el derecho nacionalsocialista tiene para hacer al mundo jurídico y la legislación racial no es más que la administración de un determinado *ordre public* nacionalsocialista que tiene por objetivo la preservación de las buenas costumbres y la protección de la sangre alemana en tanto esta fluya por las venas de los súbditos alemanes (…) el derecho nacionalsocialista no se arroga determinar quién es inglés, quién francés o quién japonés; sí insiste, sin embargo, en que la determinación de aquello que es alemán, de aquello que es substancia alemana, de aquello que es necesario para la defensa de la sangre alemana, mientras entren en consideración súbditos alemanes, es y sigue siendo asunto particular del pueblo alemán.»

Estas posiciones justamente se perciben en oposición a aquellas tesis que buscan internacionalizar nociones jurídicas a partir del reconocimiento de principios y valores universales como el de Dignidad, base esencial del derecho a la protección de datos como se verá más

adelante. En tanto, afírmese que ese propósito de universalización justamente es motivo de confrontación por Schmitt quien, citado por el mismo Saravia, afirmaba:

> «El derecho nacionalsocialista no es un derecho con vocación universalista y dirigido a toda la humanidad, y no quiere serlo» (Saravia, 2012, p. 156). «Esta última característica es la que, según Schmitt, «resalta las enormes diferencias que lo separan del derecho bolchevique que, además de internacionalista, es imperialista y agresivo, agrega Saravia» (Saravia, 2012, p. 156).

Esta serie de planteamientos restrictivos de la dignidad no solo han sido adoptados por regímenes de extrema derecha dictatorial como los del *Führer* Adolfo Hitler en Alemania o Benito Mussolini o Francisco Franco en Italia o España respectivamente. Los mismos han sido acogidos en diversos momentos de la historia por regímenes que claramente podrían ser identificados como modelos democráticos y que, a partir de su instrumentación, terminan dando lugar a lo que se podría denominar modelos jurídicos de cohabitación conceptual, es decir aquellos donde no obstante concebir la noción universal de dignidad, en ciertas circunstancias terminan aceptando ciertas prácticas que implican claras restricciones de ella, cuando no su anulación temporal.

Uno de los ejemplos de modelos jurídicos de cohabitación conceptual, es el los Estados Unidos de Norteamérica que, por ejemplo, bajo el gobierno de George W. Bush, con ocasión de los hechos del 11 de septiembre de 2001, expidió la *Authorization for Use of Military Force Against Terrorist – AUMF,* y con ella incorporó un claro concepto de dignidad restringida, incluso aún hoy vigente.

Con ocasión de la expedición de la Autorización para el Uso de la Fuerza Militar contra Terroristas, conocida por sus siglas como AUMF, en Estados Unidos de Norteamérica se puso en vigencia un marco normativo que facilitó al gobierno declarar unilateralmente a una persona como «combatiente ilegal» o «combatiente enemigo». Quienes así son calificados corresponden a:

> Una tercera categoría jurídica de detenidos definida en términos negativos, de exclusión: junto a la categoría de prisionero de guerra y a la de sospechoso de la comisión de un delito tipificado en las leyes penales (…) el cual se define por no ser ni prisionero de guerra, ni sospechoso de la comisión de un delito y que, por consiguiente, no disfruta de derecho subjetivo alguno, pues las leyes internacionales e internas solo tienen

> presente, en principio, esas dos últimas categorías (Campderrich Bravo, 2007, p. 8) (se subraya).

Es decir que, con la AUMF se creó una nueva categoría de persona que, por voluntad del gobernante, en virtud del estado de excepción y el principio de seguridad nacional, se le despoja de derechos que, bajo la *noción universal de dignidad*, sería inaceptable, pues se interpretaría como la perdida de la condición de dignidad misma que, asegura entre otros: trámites de debido proceso, presunción de inocencia, etc.

Circunstancias como estas ponen de manifiesto que la noción restringida de dignidad puede en un momento determinado estar cohabitando en el ambiente jurídico de una sociedad que para muchos constituye «paradigma democrático» y que permanentemente está expuesta a la profundización de sus radicalismo, máxime cuando en el seno de su sociedad se plantea el criterio de la responsabilidad planetaria de los Estados Unidos como gran agente de la seguridad global, pensamiento defendido por los nuevos ideólogos del neoconservadurismo norteamericano o «realismo democrático» como Charles Krauthammer quien, citado por José Luis Piñar Mañas (Piñar Mañas, 2009, p. 19), lo pone de presente en sus palabras así:

> *«We will support democracy everywhere, but we will commit blood and treasure only in places where there is a strategic necessity-meaning, places central to the larger war against the existential enemy, the enemy that poses a global mortal threat to freedom.»* (Vamos a apoyar la democracia en todas partes, pero vamos a aportar sangre y dinero solo en lugares donde hay una necesidad de significancia estratégica, sitios donde se ha mantenido largo tiempo la guerra contra enemigos existenciales, enemigos que han realizado una alianza mundial para matar la libertad).

Pero hay que decir que el caso norteamericano no ha sido el único donde la cohabitación de los conceptos de dignidad restrictiva y universal han suscitado dinámicas jurídicas controvertibles. Piñar Mañas (Piñar Mañas, 2009, p. 21) menciona algunos países donde se han adoptado o está discutiendo la necesidad de aprobar reglamentaciones restrictivas de manifestaciones de la dignidad asociadas a la protección de datos personales en relación con la auto-determinación informática, todo ello argumentados una vez más en el concepto de «Razones de Estado o Seguridad Nacional». Refiere por ejemplo que:

> en Suecia se ha aprobado una ley por la que, sin necesidad de orden judicial, se permite que los servicios secretos rastreen los correos electrónicos, llamadas telefónicas y faxes enviados al extranjero (en principio las comunicaciones nacionales no serían vigiladas). En Italia se ha planteado un

> gran debate acerca de la posibilidad o no de interceptar conversaciones privadas por razones de seguridad y se pretende poner en marcha un gran proyecto de recolección de datos, incluidos datos biométricos, de la población romaní (lo que ha merecido la crítica del Parlamento Europeo). En Alemania, en diciembre de 2008, se ha aprobado una ley que permite a la policía llevar a cabo un seguimiento y vigilancia de enorme alcance de los ciudadanos, pudiendo incluso espiar en línea los ordenadores, sin autorización judicial en «casos de urgencia (como ya sabemos, el Tribunal Constitucional alemán ya se ha pronunciado, en su Sentencia de 27 de febrero de 2008, en relación con una ley semejante del Estado de Renania del Norte Westfalia). Mientras tanto, en la Unión Europea, tras una primera posición en contra de las iniciativas que venían de Estados Unidos, se va aceptando poco a poco la adopción de medidas que pueden suponer importantes limitaciones para la libertad, los derechos fundamentales y, en particular, para la privacidad. Así, pese a la férrea oposición inicial contra los planes estadounidenses de recabar los datos de todos los pasajeros que volasen con destino o escala a/en Estados Unidos, ahora desde Bruselas se considera que tal medida es imprescindible en la lucha por la seguridad y se ha presentado una Propuesta de Decisión Marco del Consejo sobre utilización del registro de nombres de los pasajeros (Passenger Name Record –PNR–) con fines represivos, que ha merecido una muy dura contestación por parte del Parlamento Europeo, de las Autoridades de Protección de Datos de los Estados miembros, y del Supervisor Europeo de Protección de Datos. Asimismo, se estudia la posibilidad de instalar en el interior de los aviones videocámaras y micrófonos que permitan un control constante de la actividad en cabina.

Estos temas se verán aún más generalizados y agudizados a raíz de los hechos de violencia perpetradas por extremistas islamistas el 6 de enero de 2015 en París en las instalaciones de la revista Charlie Hebdo y la lucha global de la OTAN en contra del Estado Islámico.

El peligro que entraña entonces la aceptación jurídica de la noción de *dignidad restringida,* se asocia a la eventual incorporación de dicho pensamiento en la racionalidad burocrática, que en términos de Weber, expresa en la mayoría de los casos los fines de las élites dominantes más que el interés general de los asociados de un Estado, generándose por ello una clara asimetría entre el individuo común, frente a las grandes corporaciones. Recuérdese que al amparo del interés general y sobre todo de la «Razón de Estado», fácilmente se llega, como se ha visto, a la «justificada» y además «legal» supresión de elementos esenciales de la dignidad humana como lo son por ejemplo el derecho a la intimidad y por su puesto la protección de los datos personales, pero lo que puede ser más grave, al desconocimiento de

garantías procesales cuya supresión vulneran el derecho de defensa, exponiendo al ser humano a su degradación.

Ante esta crítica que genera una cierta distancia de tal línea de pensamiento, resulta oportuno aproximar las *nociones universales de dignidad* que se han contrapuesto a las acabadas de referir.

2.2.2 LA NOCIÓN UNIVERSAL DE DIGNIDAD

Parte de considerar que entre los seres humanos existe un factor común a todos que, haciéndoles diferentes de los demás seres vivos, convierte a las personas naturales todas iguales entre sí, no obstante las diferencias que en últimas lo individualizan, las que en el desarrollo del presente trabajo se denominan singularidades.

Hay que empezar por anotar que, no obstante la coincidencia que se da entre las diversas manifestaciones universalistas, justamente el referido principio de igualdad que explica la condición de dignidad del ser humano ha tenido matices diversos, según sean los contenidos que lo explican.

Las diversas vertientes que de este pensamiento universalista se han desarrollado, susceptibles de agruparse atendiendo distintos criterios, para el presente caso basado en el contenido del factor constitutivo del principio de igualdad, constituyen avances significativos en el camino del pensamiento humanista, implicando, unos u otros, tránsitos recorridos no necesariamente cronológicos, para lograr los niveles que en el lenguaje moderno el concepto universal de dignidad ha alcanzado, tal como se presenta a continuación:

2.2.2.1 **Vertiente Teológica**

Un primer grupo podría estar representado por los pensamientos teosóficos. Se enmarcan dentro de esta vertiente aquellas líneas del pensamiento que estriban su fundamentación en la creencia de un ser superior a quien se le atribuye la creación del universo y con él, por lógica, la de los seres humanos. Conciben entonces la dignidad como un atributo heredado del Creador quien infunde a todos los hombres y mujeres su «imagen y semejanza» al momento de su surgimiento. Esta concepción está claramente presente en todas las religiones de

origen judeo-cristianas. Al respecto señala Torralba i Rosselló (Torralba i Roselló, 2005, p. 251) que

> En efecto, tanto en la Doctrina Social de la Iglesia, desde León XIII hasta Juan Pablo II, como en el conjunto de la tradición teológica cristiana, el ser humano es contemplado como el ser más digno de la creación material, como lo más perfecto que subsiste en la naturaleza (en palabras de Santo Tomás de Aquino), por el hecho de haber sido creado a imagen y semejanza de Dios tal y como se expresa en el primer libro de la Biblia.

Así lo afirma en la C. 90, a. 3, refiriendo el Génesis 1,27 Tomás de Aquino quien señala que «Dios creó al hombre a su imagen. El hombre es imagen de Dios en cuanto al alma» (Aquino, 2001, p. 813). Sin embargo, deberá reconocerse que para Tomás de Aquino, esta concepción universalista de la dignidad, si bien se distancia de las claramente restrictivas consideraciones clásicas platónicas y aristotélicas, no logra su total desvinculación de aquellas pues, de alguna manera, no obstante reconocerle la calidad de dignidad a todas las personas por participar del proceso de creación divina e infusión del alma desde su creador, admite que puede darse un mayor o menor nivel de dignidad según las personas a quienes se refiera. Así por ejemplo se advierte, en la C. 59, a. 3, que «los ángeles tienen mayor dignidad que los hombres» (Aquino, 2001, p. 556) y estos mayor que las mujeres como refleja en el desarrollo de la C. 92, a. 2, al señalar que

> «No habría organización en la sociedad humana si unos no fueran gobernados por otros más sabios. Este es el sometimiento con el que la mujer, por naturaleza, fue puesta bajo el marido; porque la misma naturaleza dio al hombre más discernimiento» y agrega que «Fue conveniente que en la primera institución de las cosas, la mujer, a diferencia de los demás animales, fuera formada del hombre. 1) En primer lugar, para dar así mayor dignidad al primer hombre, el cual, siendo imagen de Dios, él mismo fuera el principio de toda su especie, como Dios es principio de Todo el universo (Aquino, 2001, p. 824).

Sin lugar a dudas estas posiciones tomistas constituyeron un avance significativo en el camino hacia el humanismo, pero sin que alcanzara la suficiente condición como para expresar a plenitud un concepto de la dignidad con connotaciones verdaderamente universalistas.

Fue por ello que, doscientos años más tarde, de frente a las nuevas realidades de la geopolítica mundial que pusieron de manifiesto interrelaciones con las comunidades nativas del «nuevo mundo», estas concepciones escolásticas fueron replanteadas aun dentro de la misma línea clerical. Pensadores, por ejemplo, como el padre Fray Barto-

lomé de las Casas, no obstante su base teosófica, se separaron del pensamiento tomista y acudiendo a dialécticas racionalistas muy propias del naturalismo, defendieron el concepto de dignidad de los indígenas del «nuevo mundo» y con ello la dignidad sin distingo alguno para todas las personas. Así lo pone de presente Emilio García García (García García, 2011) al afirmar que:

> Bartolomé de las Casas argumentará la dignidad del hombre por ser creatura de Dios, pero también por sí mismo, ya que las naturalezas creadas tienen autonomía propia. Así defenderá la dignidad de los indios con argumentos escolásticos y también propios del renacimiento y humanismo. Para Bartolomé de Las Casas, el hombre, precisamente por su naturaleza, tiene unos derechos naturales. En el plano filosófico, el hombre, por su naturaleza racional y volitiva, tiene una dignidad que le hace acreedor de determinados derechos de forma connatural e inalienable. En el plano teológico, la dignidad le viene dada por ser criatura de Dios, a su imagen y semejanza. Ambos planos, el natural y el revelado, lo comparten todos los hombres que, en su dignidad, son todos absolutamente iguales, como miembros todos de la especie humana.

En similar línea del padre de las Casas encontramos en la actualidad al filósofo latinoamericano actualmente Provincial de la Comunidad Jesuita en Colombia, Francisco de Roux-Rengifo S. J. (De Roux-Rengifo, 2009), quien de manera muy precisa manifiesta que el concepto de dignidad para los creyentes no es una cualidad que admita graduación alguna. De hecho ni siquiera es condición susceptible de evolución. Afirma que la dignidad se tiene por razón de ser humanos, y advierte que

> Nosotros no podemos desarrollar la dignidad, la dignidad está dada totalmente en cada ser humano desde el momento en que nace; desde el punto de vista cristiano, tiene el misterio del amor de Dios desde siempre y para siempre. Para quienes somos creyentes, eso afirma la grandeza humana (De Roux-Rengifo, 2009).

Sin duda, hay que reconocer que el aporte que realizó el cristianismo a la construcción de la noción universal de la dignidad ha sido de gran significancia, independiente de las realidades acaecidas durante la edad media que, pareciendo un contrasentido, pudieran argumentar en contra de lo aquí afirmado. Pasar de una época de reflexiones ius-filosóficas donde claramente eran éticos y legales los modelos esclavistas que presuponían la desigualdad como elemento natural, a este nuevo estadio del pensamiento que proclamó la naturaleza de iguales de los seres humanos, constituyó la piedra sobre la cual se se-

guiría edificando la línea universalista del concepto de dignidad. Incluso se debe sumar a lo afirmado el saber que las posturas modernas de las altas jerarquías de la Iglesia Católica han ya superado las nociones de dignidad relativista, tal como se desprende de las palabras del Papa Juan Pablo II (Juan Pablo II, 2011) cuando afirmaba

> Hemos de situarnos en el contexto de aquel «principio» bíblico según el cual la verdad revelada sobre el hombre como «imagen y semejanza de Dios» constituye la base inmutable de toda la antropología cristiana. «Creó pues Dios al ser humano a imagen suya, a imagen de Dios le creó, macho y hembra los creó» (Gén. 1, 27). Este conciso fragmento contiene las verdades antropológicas fundamentales: el hombre es el ápice de todo lo creado en el mundo visible, y el género humano, que tiene su origen en la llamada a la existencia del hombre y de la mujer, corona todo la obra de la creación; ambos son seres humanos en el mismo grado, tanto el hombre como la mujer; ambos fueron creados a imagen de Dios. Esta imagen y semejanza con Dios, esencial al ser humano, es transmitida a sus descendientes por el hombre y la mujer, como esposos y padres: «Sed fecundos y multiplicaos y henchid la tierra y sometedla» (Gén. 1, 28). El Creador confía el «dominio» de la tierra al género humano, a todas las personas, tanto hombres como mujeres, que reciben su dignidad y vocación de aquel «principio» común.

A estos planteamientos judeo-cristiano surgen contrapuestas argumentaciones desde los escenarios mismos de lo teosófico, como por ejemplo con las creencias hinduistas teístas. Para estas corrientes religiosas la dignidad no es condición exclusiva del ser humano sino cualidad de todo lo creado como quieran que su origen común es el Brahman fecundado por Krisna. Así se expresa en el *Bhagavad Gita* (Majabhárata) al señalarse que: «La sustancia material total, llamada Brahman, es la fuente del nacimiento, y es ese Brahman lo que Yo fecundo, haciendo posible el nacimiento de todos los seres vivientes…» (Viasadeba, 3000 a de C., p. Bg 14.3). Así es como el filósofo hinduista Rabindranath Tagore (Tagore, 2002), retomando tal expresión del Gita, en su poesía Flujo de Vida, expresa que

> El mismo flujo de vida que corre por mis venas día y noche, corre a través del mundo y danza en una rítmica dimensión. Es la misma vida que estalla en alegría a través del polvo de la tierra en incontables briznas de hierba y rompe en tumultuosas olas de hojas y flores.

Cabe señalar que este tipo de vertientes del pensamiento están presentes de alguna manera en nuestras culturas ancestrales latinoamericanas, hoy con pretensiones de incorporación a ordenamientos jurídicos como el Boliviano que, en el preámbulo de la Constitución

Política del Estado Plurinacional de Bolivia se hace referencia a la Madre Tierra o *Pachamama* en quechua, como una especie de invocación del origen de lo que existe o causa común creadora y por tanto fuente de igualdad entre todas las cosas y seres vivos. Obviamente hay que advertir que el desarrollo normativo posterior, enfático en materia de regulación de aspectos ambientales y particularmente el agua a la cual casi terminan dando una naturaleza de sujeto de derechos, lejos de aproximarse a las vertientes hinduista, cosifica el resto de la naturaleza en favor del ser humano, evidenciando en últimas, no obstante su pretensión discursiva, las raíces del pensamiento judeocristiano, distante en estos elementos de la culturas raizales de nuestra América latina.

Ahora bien, hay que decir sobre estas posiciones fundamentadas en elementos teosóficos (judeocristianas, hinduistas, musulmanas, etc.) que, no obstante sus tintes universalista, adolecen justamente de esta cualidad en tanto que al partir del reconocimiento de un dogma de fe (entiéndase aquellos argumentos no susceptibles de explicación racional) como lo es la existencia de uno o varios seres superiores y creadores, constituyen, para quienes no profesan la respectiva fe, una *razón* de exclusión que impediría por tanto la invitación a la aceptación racional del planteamiento expuesto en torno a la dimensión de la dignidad, motivo por el cual se obliga a la búsqueda en otras de las vertientes que esta tendencia universalista provee.

2.2.2.2 **Vertiente racionalista**

Esta línea del pensamiento, abandonando las míticas argumentaciones religiosas, busca en el ejercicio dialéctico y los consensos lingüísticos, la explicación de los elementos que caracterizan el factor de igualdad, esencia de la dignidad, en su ejercicio racional de las personas. Argumentan entonces que la igualdad de los seres humanos se fundamenta en el reconocimiento de la *facultad racional* que, en virtud del libre albedrío (concepto heredado de las vertientes teosóficas y especialmente de las judeocristianas, como lo evidencia Tomás de Aquino en la *Suma Teológica*, C. 83, a. 1 ad 4) (Aquino, 2001), les permite escoger, con categorías éticas de valoración, el proceder a ejecutar, es decir, una opción de escoger la acción o la omisión entre las varias que le presente su circunstancia. Se trata entonces, podría afir-

marse, ya no de una concepción ético-religiosa sino ético-racional la que se adopta para efectos de explicar la igualdad de los seres humanos y a partir de ella la condición universal de la dignidad.

En términos de Kant, Citado por Torralba i Roselló (Torralba i Roselló, 2005, p. 252), uno de los representantes más significativos de esta tendencia del pensamiento, la dignidad del ser humano está dada en función de la igualdad que se origina de su

> capacidad humana de elección moral. Es decir, los seres humanos podían variar en cuanto a la inteligencia, la riqueza, la raza y el sexo, pero todos ellos eran igualmente capaces de actuar o no actuar conforme a la ley moral.

Este planteamiento lleva a considerar que, siendo el ser humano un ser igual por su común condición ético-racional, en palabras del mismo Kant, citado por Pelé (Pelé, Una Aproximación al concepto de Dignidad Humana, 2004, p. 12),

> la humanidad misma es dignidad: porque el hombre no puede ser utilizado únicamente como medio por ningún hombre (ni por otros, ni siquiera por sí mismo), sino siempre a la vez como fin, y en esto consiste precisamente su dignidad (la personalidad) en virtud de la cual se eleva sobre todas las cosas (...).

Hay que señalar que, como quedó anticipado, por esta línea del pensamiento discurre incluso un importante sector de la Iglesia Católica que encuentra en el ya mencionado sacerdote De Roux uno de sus mejores expositores. De Roux (De Roux-Rengifo, 2009) define y explica la dignidad, a la mejor manera Kantiana, en los siguientes términos:

> (…) La sociedad humana se fundamenta en el respeto que nos tengamos mutuamente los unos a los otros, en lo que la ética liberal desarrolló con las ideas de Immanuel Kant: trata a los demás como tú quieres que los demás te traten a ti; no uses a nadie como medio para ningún fin económico ni político ni de ninguna otra clase, porque cada ser humano es un fin en sí mismo. Esa dignidad –que no la recibimos del Estado ni la recibimos de la sociedad, sino que simplemente la tenemos por ser seres humanos– no puede crecer; igual la tiene un niño del Chocó que el Presidente de la República. Pero lo que sí tenemos que hacer económicamente, con ciencias económicas, administrativas y contables, es crear las condiciones para que un pueblo pueda celebrar su dignidad, compartir su dignidad, proteger su dignidad. Hay un caso muy interesante, que utiliza Muhammad Yunus, el premio Nobel de Paz de 2006, que creó el Grameen Bank, cuando él dice: Mire, es parecido a lo que pasa con un bonsái de mango y un gran árbol de mango: usted ve el árbol de mango inmenso que puede alcanzar 30 metros de altura, se llena de mangos por todas partes y al lado, usted puede tener

> en un bonsái de solo 30 centímetros de altura un manguito chiquitico, porque lo ha mantenido dentro de un bonsái. Pero tienen la misma esencia, la misma savia por dentro; digamos que tienen la misma dignidad, pero el que está en el bonsái, está así porque le cortamos las raíces, porque lo encajamos dentro de una cajita, porque no lo dejamos expresar la magnitud de lo que ese árbol es y lo mantuvimos encerrado.

Frente a esta línea del pensamiento racionalista se han levantado voces que plantean como riesgo del enfoque eminentemente racionalista kantiano, podría dejar abierto el discurso para que, así no sea su propósito, se pueda llegar, argumentativamente hablando, a excluir de la condición de dignos a aquellas personas que por diversas circunstancias se encuentren privadas del uso de razón. Tal sería el caso de los afectados por trastornos mentales, sujetos en estado de vida vegetativa, los que están por nacer, etc. Por este motivo, reconociendo el valor de lo aportado por tal vertiente kantiana, en el ejercicio por superar la argumentación metafísica y el riesgo de la dialéctica reduccionista, se percibe la necesidad de buscar otras líneas del universalismo que faciliten más sólidamente la dimensión conceptual de la dignidad que satisfaga a los propósitos del presente trabajo.

2.2.2.3 **Vertiente racionalismo naturalista**

Esta corriente del pensamiento construye el concepto de dignidad basada en un principio de igualdad de los seres humanos a partir del reconocimiento de sus características genéticas o biológicas, susceptibles estas de identificación incluso con la mera observancia. Estas características hacen al ser humano diferente de los demás seres vivos.

Hay que recordar que tal propósito argumentativo estriba en la búsqueda de una frontera que permita, desde lo ius-filosófico, señalar cuándo se entiende trasgredida o no la dignidad de una persona, para el caso del presente trabajo, por ejemplo, con la violación de sus datos personales. Este ejercicio no ha resultado sencillo tal como lo advierte Alberto Oehling de los Reyes, al afirmar que: «Es difícil encontrar una unidad de medida de la que podamos partir para observar si se ha producido una lesión de la dignidad» (Oehling de los Reyes, 2010, p. 128).

Una aproximación muy interesante en el propósito de señalar los linderos de valoración sobre la trasgresión de la dignidad, lo ha constituido también el intento de afincar tal marco en el dolor. En esta lí-

nea Oehling de los Reyes refiere (Oehling de los Reyes, 2010, p. 128), por ejemplo, quien ha manifestado:

> El dolor humano, el sufrimiento y el padecimiento de la persona, puede servir a tal efecto, como un, por así decirlo, parámetro objetivo-natural de medida. El dolor es –siempre y cuando se tengan las capacidades cognitivas plenas y no se sufra ninguna psicopatía– una cualidad «innata» y «universal, es lo que a todos une» y se define como «una experiencia sensorial y emocional desagradable asociada o no a una lesión física.

Estas anotaciones de Oehling encuentran sustento en trabajos que desde el campo de la neurociencia se han estado aportando en los últimos tiempos. Por ejemplo los de Trujillo Mariel (Trujillo Mariel, 2009, p. 49), señaló que:

> El dolor es una expresión natural de advertencia, cuya percepción es singular y específica en cada sujeto. Sentir dolor a nivel orgánico constituye un signo de daño. El dolor se enmarca dentro de los criterios fundamentales que identifican a la inflamación. Cuando el dolor se percibe, significa que fueron vencidas todas las reservas de defensas.

Sin embargo, algunos plantean que en el ser humano, a diferencia del resto de los seres vivos, el dolor logra una expresión superior a través del denominado dolor social, sobre el cual se han adelantado importantes desarrollos en la Universidad de Chicago. En dicha universidad fue dado a conocer en enero de 2013 el *paper* titulado «El estudio del impacto del contexto social en la percepción del dolor en los demás es importante para la comprensión del papel de la intencionalidad en la sensibilidad interpersonal, la empatía y el razonamiento moral implícito» (Akitsuki & Decety, 2013). Se afirma en este estudio que el ser humano está biológicamente programado para, además de sentir su propio dolor físico o psicológico, también sufrir como propio el dolor de los demás –el que denominan dolor social– convirtiéndose en un «mecanismo estructurador del proceso de racionamiento moral» (Akitsuki & Decety, 2013).

Esta sugestiva argumentación del dolor como frontera, a la cual cabría similar crítica de la efectuada a la de la vertiente racionalista en relación con las personas con afectaciones neurológicas, tiene adicionalmente como debilidad argumentativa la circunstancia de considerarse que el dolor (incluso en la dimensión del dolor social) es de exclusiva naturaleza humana. Ya desde mediados del siglo XIX Charles Darwin (Darwin, 1852, pp. 84-85) había advertido de las emociones tanto en los humanos como en los animales y en particular las asocia-

das al dolor. Es decir que, como el proceso neurológico del dolor es común a muchas de las especies vivas incluida los humanos, no pudiera argumentarse como elemento tipificador y por tanto factor diferencial entre estos y las demás criaturas de la naturaleza. Por esta razón, se ve la necesidad de auscultar en otras líneas del pensamiento que permitan argumentar la existencia de la dignidad universal a partir de presupuestos efectivos de igualdad de los seres humanos exclusivamente.

En este propósito, se trae a referencia a Francis Fukuyama quien, citado por Torralba i Roselló (Torralba i Roselló, 2005, p. 254), refiriéndose al factor X como aquel componente diferenciador de los humanos para con las demás especies, como lo era el origen divino en las escuelas Teológicas o el razonamiento ético en el caso de los racionalistas, lo define así:

> La complejidad es un dato empírico y biológico que todo ser humano puede reconocer, sin necesidad de realizar el salto de la fe. No es posible objetar nada, pues, a su juicio, el ser humano es el más complejo del orden natural y, por ello, el más capaz de vida emocional, mental, de actividad artística o científica. Esta complejidad es la que permite al ser humano resolver satisfactoriamente en cada contexto y en cada época su extrema vulnerabilidad física.

Este planteamiento de Fukuyama sobre el «Factor X» como elemento diferenciador de los seres humanos en relación con los demás seres vivos, constituirá la base de la argumentación universalista de la dignidad que se adopta para todos los efectos del presente trabajo y según la cual, se reconoce que un ser humano despojado de cada uno de sus elementos biológicos diferenciadores (color de piel, ADN, iris, huella decadactilar o cabello, altura, edad, etc.), considerado sin tener en cuenta sus distintos niveles de conocimiento y de comprensión racional de la realidad (ilustrados o no, conscientes o no), despojados de las condiciones externas como riqueza u honores, se le considera idéntico en esencia a los demás, pero a su vez diferentes de cualquiera otra especie.

Justamente esa esencia diferenciadora es la que hace a los humanos *potencialmente* seres hacedores de historia. Y, se hace énfasis en la condición de *potencialidad*, para anticipar respuesta a las críticas que en su momento cupieron al racionalismo y que en ningún sentido pudieran pretenderse contra esta vertiente naturalista.

De esta forma, se advierte que la potencialidad que se predica, se hace tanto del ignorante como del ilustrado, del rico como del pobre, pero de igual forma de quien ostenta adecuada condición de salud

como quien, por estar privado de ella, pueda carecer incluso de estado de conciencia.

En palabras de Fromm, es la esencia existencial del ser humano según la cual «la vida del hombre no puede "ser vivida" repitiendo el patrón o modelo de su especie: tiene que vivirla él» (Fromm, 1964, p. 27), enfrentado permanentemente a la «necesidad de encontrar soluciones siempre nuevas para las contradicciones de su existencia, de encontrar formas cada vez más elevadas de unidad con la naturaleza, con sus prójimos y consigo mismo» (Fromm, 1964, p. 28) dejando, a diferencia de las demás especies, la huella de su tránsito por el tiempo y el espacio.

Esa esencia particular y propia de la raza que nos hace seres potencialmente capaces de «desarrollar actividades como el pensar, el amar y crear» como afirma Torralba i Roselló (Torralba i Roselló, 2005, p. 259) y a lo cual puede agregarse: potencialmente capaces de construir la fantasía para sí y para otros en busca de la felicidad colectiva, es justamente el factor diferenciador para con las demás especies, pero a su vez igualador entre la especie misma.

Estos rasgos comunes que potencialmente igualan la especie humana y le diferencia de las otras, es justo la esencia misma del principio de igualdad, además de explicación y justificación racional de la existencia del Estado, en cuanto que este debe surgir de los iguales que lo acuerdan o adoptan, y para la conservación de tal condición, pues de proceder con fin distinto, se estaría contrariando la condición natural que se señala. En tal sentido expresaba Rousseau (Rousseau, 1999, p. 27) cuando advertía, en el Contrato Social, que el Estado

> … no es más que una persona moral cuya vida consiste en la unión de sus miembros, y si el más importante de sus cuidados es el de la propia conservación, preciso le es una fuerza universal e impulsiva para mover y disponer de cada una de las partes de la manera más conveniente al todo.

Es decir que, en otras palabras, el Estado debe ser imaginado, creado, organizado, administrado, y en últimas justificado, en cuanto garante del principio natural y universal de Dignidad que se fundamenta en la igualdad que naturalmente poseen, de manera exclusiva los miembros de la especie humana, por ello, siempre las reglas jurídicas que cualquier Estado desarrolle para el logro de sus fines habrán de estar sometidas a aquella.

2.3 DIGNIDAD COMO DERECHO SUBJETIVO Y SOPORTE DEL HÁBEAS DATA

Precisado como ha quedado el principio de igualdad basado en la esencia diferenciadora advertida, se sigue de ello necesariamente que siendo iguales los seres humanos no le es dado a ninguno someter como instrumento a otro, es decir que, de la esencia natural igualitaria surge, en sentido contrario a la prohibición de la cosificación del hombre, el pleno reconocimiento de su condición de seres libres. De ello se deriva por tanto la inadmisibilidad de que en perjuicio de otro interés diferente que el común (el que no necesariamente coincide siempre con el de las mayorías), pudiera alguno o algunos someter a condición de desigualdad (esclavitud, explotación, segregación, aislamiento, etc.) uno cualquiera de sus congéneres, condición reprochable a la luz de la racionalidad expresada, pues, como argumenta el profesor Dworkin

> El principal valor de la libertad es el valor de la elección y de la capacidad de dirigir la propia vida, y si empieza su carrera como esclava, nunca va a poder recuperar más que una cantidad simbólica de ambos (Dworkin, Una cuestión de principios, 2012).

Es decir que la doble condición de igualdad y libertad, es en sí misma la única condición adecuada a la naturaleza de la especie humana, llamada a conservarse por el contexto general de la sociedad toda ella, en cualquier tiempo o espacio. Esta condición es la que se propone denominar *condición de dignidad*.

En consecuencia, la *condición de dignidad* se proclama de una y solo una de las múltiples especies vivas del planeta, esto es la especie humana, lo que permite y da validez al imperativo categórico de facilitar que las demás especies puedan ser cosificadas (siempre, claro está, conforme *a su* naturaleza y *a la* naturaleza, en razón del deber generacional y por tanto ambiental que ello entraña), es decir convertidas en medios, condición jamás nunca aceptable para ninguno de los miembros de la especie humana.

Asumida, para efectos del presente trabajo, la dignidad en su *noción universal*, tal como se ha afirmado, queda ahora por expresar que esta, en cuanto *condición*, presupone una relación jurídica que vincula a cada uno de los individuos entre sí y al individuo, particularmente considerado, para con los Estados. Esta circunstancia, tal

como se muestra en la siguiente figura es la que nos permite señalar que la *condición de dignidad* posee una doble calidad, esto es como principio (fundante del Estado como ha quedado dicho) y como derecho subjetivo. En esta última calidad como se demuestra adelante, la dignidad presenta una doble dimensión, esto es la dimensión activa y la dimensión pasiva.

Figura 1. *Relación jurídica del derecho de dignidad*

«Diagrama de la relación jurídica entre el titular de la dignidad (parte activa) para con los congéneres y Estados (parte pasiva).»

«Entre el titular de la dignidad (parte activa) por una parte, y, por la otra los congéneres y los Estados (parte pasiva) se establece una relación jurídica que surge por el solo hecho del nacimiento y continúa hasta la muerte.»

2.3.1 LA DIMENSIÓN ACTIVA DE LA DIGNIDAD

Esta dimensión de la condición de dignidad implica su reconocimiento como derecho subjetivo en cabeza de cada uno de los miembros de la especie humana que les faculta a exigir para sí y para todos, una vida en condiciones tales que le sea garantizada su condición de libres e iguales.

Quepa reseñar que al hacerse referencia a la condición de dignidad como derecho subjetivo, se hace mención a la noción de derecho subjetivo en sentido estricto, que en palabras de H. Maurer, referido por Rodolfo Arango Rivadeneira (Arango Rivadeneira, El concepto

de derechos sociales fundamentales, 2012, p. 9), se entiende generalmente como «el poder legal reconocido a un sujeto por medio de una norma legal, para la persecución de intereses propios mediante la exigencia a otro de hacer, permitir u omitir algo».

En este orden de ideas, cabe afirmarse que el derecho subjetivo de la *condición de dignidad* en sentido estricto, en términos de Arango Rivadeneira (ibídem), se pregona por cuanto existen sus elementos constitutivos, esto es una norma jurídica, un poder jurídico (es decir una posición jurídica) y una obligación jurídica (sobre este elemento se aborda más adelante al desarrollarse la dimensión pasiva de la dignidad) así:

1. La norma jurídica: Valga afirmarse que en cuanto se refiere a la norma jurídica basta con traer a colación las siguientes disposiciones jurídicas que ponen de presente la existencia de esta primera característica del derecho subjetivo de la *condición de dignidad*:

— Declaración Americana de los Derechos y Deberes del Hombre del 2 de mayo de 1948. Proclamó, en sus consideraciones, la dignidad humana como un valor universal y la obligación del Estado de protegerla en los siguientes términos:

CONSIDERACIONES: Que los pueblos americanos han dignificado la persona humana y que sus constituciones nacionales reconocen que las instituciones jurídicas y políticas, rectoras de la vida en sociedad, tienen como fin principal la protección de los derechos esenciales del hombre y la creación de circunstancias que le permitan progresar espiritual y materialmente y alcanzar la felicidad… (http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp).

Con estas afirmaciones, toda discusión acerca del reconocimiento de la dignidad de las personas naturales y por tanto de la titularidad de derechos esenciales estaba superada. La condición de miembro de la raza humana, quedó establecida como el único elemento, de suyo eminentemente natural, necesario para pregonar el amparo del valor supremo de la dignidad. En el preámbulo de la misma declaración se reafirmó el principio superior de la dignidad en los siguientes términos: «PREÁMBULO: Todos los hombres nacen libres e iguales en dignidad y derechos» (http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp). Evidentemente el valor de la dignidad se erigió como un límite al actuar del Estado y de los demás conciudadanos. A

partir de este momento histórico, toda actuación pública o privada, entre los países de América, que violentara este principio de dignidad, estaría enmarcado en una clara violación de los derechos esenciales, más tarde denominados fundamentales.

— Declaración Universal de Derechos Humanos del 10 de diciembre de 1948, que por su naturaleza no requiere de ley para incorporarla en la normativa nacional de los Estados miembros como Colombia, desde su Preámbulo proclama la dignidad como base de la libertad, la justicia y la paz en el mundo. Y en su artículo 1.º advierte «Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros». Es decir, se reconoció el principio de dignidad humana, como pilar de las sociedades democráticas y de los Estados modernos, a partir de tal momento con una dimensión global.

— Ley 16 de 1972 (diciembre 30) por medio de la cual se aprueba la Convención Americana sobre Derechos Humanos «Pacto de San José de Costa Rica», firmado en San José, Costa Rica, el 22 de noviembre de 1969». En su artículo 5.º se reconoce la dignidad como inherente al ser humano y en el artículo 11 se señala el derecho a la protección de la dignidad.

— Ley 74 de 1968 (diciembre 26) por la cual se aprueban los «Pactos Internacionales de Derechos Económicos, Sociales y Culturales, de Derechos Civiles y Políticos, así como el Protocolo Facultativo de este último, aprobado por la Asamblea General de las Naciones Unidas en votación unánime, en Nueva York, el 16 de diciembre de 1966». Desde los considerandos de dichos pactos, al igual que en su artículo 31, se reconoce la dignidad como inherente a la persona humana y fuente de los demás derechos. En su artículo 13 obliga a los Estados a orientar la educación hacia «el pleno desarrollo de la personalidad humana y del sentido de su dignidad».

— Ley 70 de 1986 (diciembre 15) «Por medio de la cual se aprueba la «Convención contra la tortura y otros tratos o penas crueles, inhumanos o degradantes, adoptada en Naciones Unidas el 10 de diciembre de 1984». Reconoce una vez más, como es una constante en materia de pactos y acuerdos internacionales suscritos por Colombia en temas referidos a Derechos Fun-

damentales, que de la dignidad humana surgen los demás derechos que dichos tratados buscan proteger.

2. Poder jurídico o posición jurídica: Salvadas las discusiones que los tratadistas han dado sobre la diferencia conceptual que abrigan las expresiones poder jurídico y posición jurídica como lo refiere el mismo profesor Rodolfo Arango Rivadeneira (Arango Rivadeneira, El concepto de derechos sociales fundamentales, 2012, pp. 14-22), baste para el propósito del presente ejercicio decir que, en tratándose de la condición de dignidad, a cada uno de los individuos le asiste la facultad de exigir válidamente (amparados en las normas referidas) la realización de conductas activas o pasivas para garantizar su condición de dignidad. Es decir, que los seres humanos, en razón de su condición de dignidad inherente, pueden exigir a otros (los demás individuos y los Estados todos) unos comportamientos positivos (deber de acción) y/o negativos (deber de abstención) orientados a lograr, restablecer o conservar dicha condición.

2.3.2 LA DIMENSIÓN PASIVA DE LA DIGNIDAD

3. Obligación jurídica: El tercer elemento estructurante de los derechos subjetivos, en términos de Arango Rivadeneira, corresponde a la obligación jurídica, es decir la dimensión pasiva de la dignidad que, para efectos de la condición de dignidad, destaca dos manifestaciones:

En primer lugar, el *deber de solidaridad,* radicado en cabeza de todos y cada uno de los miembros de la especie humana, entendida esta obligación jurídica como el deber individual y colectivo de la acción y la omisión orientada al aseguramiento de la existencia digna de todos y cada uno de los miembros de la especie, razón que explica y ordena, entre otras, la participación tributaria como presupuesto básico de la redistribución justa de la riqueza y,

En segundo lugar, el *deber de justicia*, radicado en cabeza todos y cada uno de los Estados, comprendido como la obligación explícita e implícita que les asiste de proceder, activa y pasivamente, en el propósito de asegurar las condiciones de libertad y de igualdad, las que a su vez han de entenderse concomitantemente como fin y límite de su propio actuar.

Puede entonces afirmarse que en tratándose de la *condición de dignidad*, por evidenciarse la existencia de los tres presupuestos cons-

titutivos del derecho subjetivo, se le reconoce tal calidad, surgiendo consecuentemente la necesidad de resolver el interrogante acerca de cuál es el núcleo esencial del derecho subjetivo de la dignidad.

2.4 NÚCLEO DE LA DIGNIDAD

De lo expuesto hasta ahora se colige que, de una sociedad ideal donde todos y cada uno de los miembros se encuentran en *condición de Dignidad,* se afirmaría hallarse estructurada bajo un modelo de *Estado de Dignidad* en cuanto que sus miembros, por cumplir efectivamente el deber de solidaridad y el Estado su deber de justicia, no tendrían que hacer valer, para sí o para otro, su *posición jurídica* ante los jueces. Sin embargo la realidad es otra. Muchos son los casos en que los miembros de una sociedad incumplen su deber de solidaridad (evasión del justo tributo, exclusiones sociales, por ejemplo) o donde el Estado no hace lo suyo en relación con su deber de justicia (prevenir o sancionar eficazmente la exclusión o redistribuir adecuadamente la riqueza, por citar un par de casos). Estas circunstancias de alteración de la *condición de Dignidad,* producen graves asimetrías sociales que obligan a ser reconocidas como violatorias de dicho principio.

En otras palabras, la condición de dignidad constituye la esencia del *Principio de Dignidad* pues, a su vez, se erige como «un estándar que ha de ser observado, no porque favorezca o asegure una situación económica, política o social que se considera deseable, sino porque es una exigencia de la justicia, la equidad o alguna otra dimensión de la moralidad» como lo podría afirmar Dworkin (Dworkin, Los Derechos en serio, 1984, p. 72).

Este *Principio de Dignidad*, que, como se advirtió fue proclamado en la Declaración Americana de los Derechos y Deberes del Hombre y en la Declaración Universal de Derechos Humanos (ambas de 1948), ha sido incorporado, en diversas Constituciones Políticas del mundo democrático, tal como ha ocurrido también en el caso colombiano donde se ha adoptado como valor, en el entendido que constituye un principio fundante del ordenamiento jurídico y por ende del Estado; como principio constitucional y como derecho fundamental autónomo Sentencia T-881 de 2002, y cuya dimensión normativa se ha concretado en asegurar al ser humano la posibilidad de construir y

desarrollar su plan de vida, ejecutarlo contando con las condiciones materiales concretas y sin que sea sometido a exclusiones o discriminaciones humillantes. En tal sentido se ha expresado recientemente la Corte Constitucional, reafirmando la ya decantada línea dogmática sobre este tema, al afirmar:

> La jurisprudencia constitucional ha sostenido que la dignidad humana, en cuanto derecho, se concreta en tres dimensiones que resultan indispensables para la vida de todo ser humano: (i) el derecho a vivir como se quiera, que consiste en la posibilidad de desarrollar un plan de vida de acuerdo a la propia voluntad del individuo; (ii) el derecho a vivir bien, que comprende el contar con unas condiciones mínimas de existencia; y (iii) el derecho a vivir sin humillaciones, que se identifica con las limitaciones del poder de los demás (...) (Sentencia T-277 de 2015).

Figura 2. *Dimensión normativa de la dignidad*

«La jurisprudencia constitucional ha reconocido tres manifestaciones dimensionales de la dignidad que deben ser garantizadas y asegurada por los Estados en virtud de su obligación de justicia y por los congéneres en virtud de sus obligaciones de solidaridad.»

En otras palabras, el *Principio de Dignidad* no tendría eficacia alguna, si el mismo no lograra alcanzar, en términos de la Corte Constitucional una dimensión normativista, esto es:

> (…) funcionalista en el sentido de completar los contenidos de aquella, con los propios de la dimensión social de la persona humana…» (Sentencia T-881 de 2002), tal como justifica la Corte Constitucional Colombiana al señalar que, «… resulta de especial importancia, al menos por tres razones: primero, porque permite racionalizar el manejo normativo de la dignidad humana, segundo, porque lo presenta más armónico con el contenido axiológico de la Constitución de 1991, y tercero, porque abre la posibilidad de concretar con mayor claridad los mandatos de la Constitución… En conclusión, los ámbitos de protección de la dignidad humana, deberán apreciarse no como contenidos abstractos de un referente

natural, sino como contenidos concretos, en relación con las circunstancias en las cuales el ser humano se desarrolla ordinariamente.

De tal forma que integra la noción jurídica de dignidad humana (en el **ámbito de la autonomía individual**), la libertad de elección de un plan de vida concreto en el marco de las condiciones sociales en las que el individuo se desarrolle. Libertad que implica que cada persona deberá contar con el máximo de libertad y con el mínimo de restricciones posibles, de tal forma que tanto las autoridades del Estado, como los particulares deberán abstenerse de prohibir e incluso de desestimular por cualquier medio, la posibilidad de una verdadera autodeterminación vital de las personas, bajo las condiciones sociales indispensables que permitan su cabal desarrollo.

Así mismo integra la noción jurídica de dignidad humana (en el **ámbito de las condiciones materiales de existencia**), la posibilidad real y efectiva de gozar de ciertos bienes y de ciertos servicios que le permiten a todo ser humano funcionar en la sociedad según sus especiales condiciones y calidades, bajo la lógica de la inclusión y de la posibilidad real de desarrollar un papel activo en la sociedad. De tal forma que no se trata solo de un concepto de dignidad mediado por un cierto bienestar determinado de manera abstracta, sino de un concepto de dignidad que además incluya el reconocimiento de la dimensión social específica y concreta del individuo, y que por lo tanto incorpore la promoción de las condiciones que faciliten su real incardinación en la sociedad.

El tercer ámbito también aparece teñido por esta nueva interpretación, es así como integra la noción jurídica de dignidad humana (en el ámbito de la **intangibilidad de los bienes inmateriales de la persona concretamente su integridad física y su integridad moral**), la posibilidad de que toda persona pueda mantenerse socialmente activa. De tal forma que conductas dirigidas a la exclusión social mediadas por un atentado o un desconocimiento a la dimensión física y espiritual de las personas se encuentran constitucionalmente prohibidas al estar cobijadas por los predicados normativos de la dignidad humana; igualmente tanto las autoridades del Estado como los particulares están en la obligación de adelantar lo necesario para conservar la intangibilidad de estos bienes y sobre todo en la de promover políticas de inclusión social a partir de la obligación de corregir los efectos de situaciones ya consolidadas en las cuales esté comprometida la afectación a los mismos. (Sentencia T-277 de 2015) (se resalta y subraya fuera de texto).

2.5 LAS SINGULARIDADES DEL SER HUMANO NEXO ENTRE DIGNIDAD Y HÁBEAS DATA

Habiéndose definido la noción filosófica y jurídica de la dignidad y teniéndose claro que según Ley 1581 de 2012, artículo 3.º, ha definido como objeto de protección los Datos Personales entendidos

como «cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables», surge preguntarse ¿cuál es la relación del *Principio de Dignidad* con el Derecho a la Protección de los Datos Personales?

Para iniciar, oportuno resulta afirmar que los datos personales constituyen ese conjunto de informaciones que, en su conjunto y/o individualmente consideradas, pueden ser asociados a una determinada o determinable persona natural. Constituyen ejemplo de ellos el nombre, su identificación (la cédula de ciudadanía para el caso colombiano), su ADN, su raza, sus gustos, sus aficiones, sus creencias, su domicilio, su inclinación sexual, etc., que lo hacen único entre los demás de su especie. A este conjunto de informaciones, por tal razón, se les denomina singularidades.

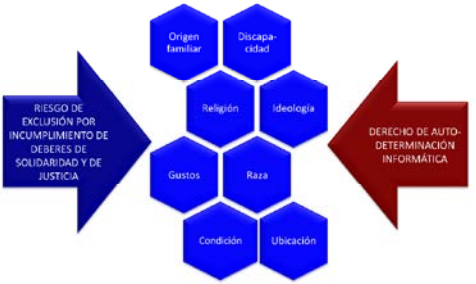


Figura 3. *Singularidades protegidas por el Hábeas Data*

«Los datos personales, como singularidades que lo son de los seres humanos, generan permanente exposición de riesgo en sociedades en condición de dignidad quebrantada, circunstancia que obliga a la expedición de normas de protección de datos personales.»

El ser humano, en cuanto individuo, en sus relaciones sociales busca por regla general el reconocimiento y aceptación de los demás, para lo cual se ve muchas veces obligado a exponer justamente las singularidades que le caracterizan y distinguen. Es el caso de quienes por ejemplo expresan inclinaciones ideológicas o teosóficas para ser aceptados por ciertos grupos políticos o religiosos, quienes se reconocen adictos al alcohol para ser aceptados en grupos de terapia para alcoholismo, igual que ocurre con otras enfermedades, o simplemente quienes manifiestan hoy en día en las redes sociales del internet sus gustos y preferencias para ser admitidos por otros como sus seguidores. Sin embargo, en ciertas circunstancias, las singularidades que un

individuo expone o pone de relieve, en lugar de ser factor de reconocimiento y aceptación, terminan constituyendo causa de exclusión como consecuencia de «conductas dirigidas a la exclusión social mediadas por un atentado o un desconocimiento a la dimensión física y espiritual» (Sentencia T-881 de 2002), como ocurre en los casos de racismo, homofobia, xenofobia, etc. En estos eventos, se identifica que «el ámbito de la intangibilidad de los bienes inmateriales de la persona concretamente su integridad física y su integridad moral» Sentencia T-881 de 2002 son vulnerados, es decir que la *condición de dignidad* es quebrantada o, en otras palabras, a la víctima de los referidos comportamientos le resulta violado o vulnerado el *Principio de Dignidad*.

Es decir que, la puesta en evidencia de las singularidades, en ciertas sociedades con disfunciones en el cumplimiento del deber de solidaridad por parte de sus miembros y/o con una deficiente manifestación del deber de justicia por parte del Estado, exponen en forma flagrante a los individuos de la especie humana a afectaciones de su dignidad y por ende de su libertad y su igualdad. Esta es la razón que obliga, en salvaguardia del *Principio de Dignidad*, reconocerle a los individuos la libertad para que, por regla general, decida compartir o no sus singularidades en el momento que su convicción lo considere necesario y conveniente, salvo ciertas excepciones que la ley consagre, casi siempre inspiradas en el interés colectivo (no de los miembros de un conglomerado en especial sino de la especie humana).

Esta correlación entre libertad y facultad de disposición de las singularidades para garantizar la igualdad, en desarrollo del principio de dignidad, culminó generando el reconocimiento del derecho a la autodeterminación informática, tal como lo advirtió la Corte Constitucional en Sentencia T-729 de 2002 , al afirmar que

> Bajo la égida del derecho general de libertad (artículo 16) y la cláusula específica de libertad en el manejo de los datos (artículo 15 primer inciso), la jurisprudencia ha reconocido la existencia-validez del llamado derecho a la autodeterminación informática.

Esta autodeterminación, como se afirmará adelante, constituye una de las manifestaciones del Hábeas Data, el que la misma sentencia del Alto Tribunal definió como:

> El derecho fundamental al Hábeas Data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualiza-

> ción, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales (…).

Definiendo la dimensión del derecho al Hábeas Data como derecho autónomo, luego de una evolución dogmática que adelante se aborda, y que en tanto se recrea en los siguientes términos:

> La Corte Constitucional ha afirmado la existencia-validez de tres derechos fundamentales constitucionales autónomos: el derecho a la intimidad, el derecho al buen nombre y el derecho al Hábeas Data. Sin embargo, el estado actual de cosas no fue siempre el mismo. El camino de la delimitación empieza en el año de 1994, con la sentencia T-229 de 1994, en la cual la Corte estableció una clara diferencia entre el derecho a la intimidad y el derecho al buen nombre. Más adelante, en el año de 1997, con la sentencia T-557 de 1997 la Corte precisó las diferencias entre el derecho a la intimidad y el Hábeas Data, después de que la relación entre ambos se había manejado como de género a especie desde el año de 1992.

De esta manera es como el Hábeas Data o Autodeterminación Informática, junto con otros derechos, como el de la Intimidad y el Buen Nombre, se identifica como un derecho subjetivo autónomo e instrumental, establecido para efectos de garantizar la protección de la naturaleza humana de los titulares cuyos datos se estén tratando, es decir su dignidad. Por tal razón, siempre que se realiza cualquier aproximación a la protección de datos personales, ya como jueces, ya como autoridades de control (la Superintendencia de Industria y Comercio en el caso Colombiano o la Agencia de Protección de datos en el caso Español, por ejemplo), ya como organización pública o privada que involucra singularidades (datos personales de personas naturales), habrá de hacerse teniendo claro que el principio que subyace en cada una de las reglas que le regulan es el *Superior Principio de la Dignidad Humana*.

3. DEL NÚCLEO A LA PERIFERIA, EL TRASPLANTE NORMATIVO DE LA PROTECCIÓN DE DATOS

3.1 ANTECEDENTES HISTÓRICOS

Hasta antes de la segunda guerra mundial, el concepto de derecho a la protección de datos personales como tal, no había sido incorporado en la agenda temática del universo jurídico. Los ciudadanos todos, de manera desprevenida, realizaban permanentemente un intercambio de información personal, sin detenerse a efectuar reparo alguno en los riesgos que ello entrañaba. El domicilio, la edad, el estado de salud, la afiliación partidista, las inclinaciones sexuales o incluso el auto-reconocimiento como perteneciente a una determinada raza o etnia, eran intercambiados y almacenados sin exigencia normativa que le regulara. Lejos se estaba aún de la implementación de sistemas de identificación personalizada a partir de los patrones de ADN o los sistemas de autenticación biométrica a partir de las huellas dactilares, del iris, la córnea, etc. que harían aún más complejo el asunto. En aquel momento de la historia, tratar los datos personales no implicaba preocupación mayor. Para ese entonces, no existía una conciencia clara de la relación entre datos personales y riesgos de afectación de la dignidad humana como consecuencia de la utilización indebida de aquellos. De hecho, aún no se había materializado tan siquiera el concepto de la dignidad humana como principio superior en la normativa jurídica de las naciones.

Tras finalizar la segunda guerra mundial, con ocasión de los juicios de Núremberg, descorridos los velos de lo acontecido bajo el accionar del régimen nazi, se encendieron las primeras alarmas sobre la necesidad de poner límites claros al actuar de los Estados y por supuesto de los individuos mismos en relación con la dignidad de las personas. Como consecuencia de ello, se empezó a establecer barreras al manejo de la información personal, como quiera que en muchos casos su utilización indebida trajera consigo claras violaciones de los derechos humanos. Constituye ejemplo de lo acaecido en la Alemania nazi, en el campo de la salud, hechos como los narrados por el médico y filósofo Horacio Riquelme (Riquelme U, 2004, pp. 25-27), según

el cual, «antes de ser muertos los niños sin valor para vivir, podían ser objeto allí de intensas investigaciones fisiológicas y psicológicas, cuyos resultados podían ser comparados con los cerebros extraídos posteriormente…».

Otra práctica ejecutada por el régimen nazi fue la «Acción T4» que implicaba, como lo describe el mismo autor, como preparación para la guerra, la liberación de camas a partir de la aplicación de la asfixia con anhídrido carbónico como método de muerte para aquellos pacientes que eran identificados como «sin valor para vivir».

Los macabros descubrimientos allí evidenciados pusieron de relieve la necesidad de prohibir que, bajo el amparo de «la ley», se permitiera la ejecución de actos de ignominia en contra de cualquier ser humano. Así mismo se puso de manifiesto que muchos de aquellos actos que violentaron la dignidad de judíos, gitanos, enfermos terminales, homosexuales, etc., se había facilitado en función de la utilización de los datos personales que el régimen nazi había recolectado.

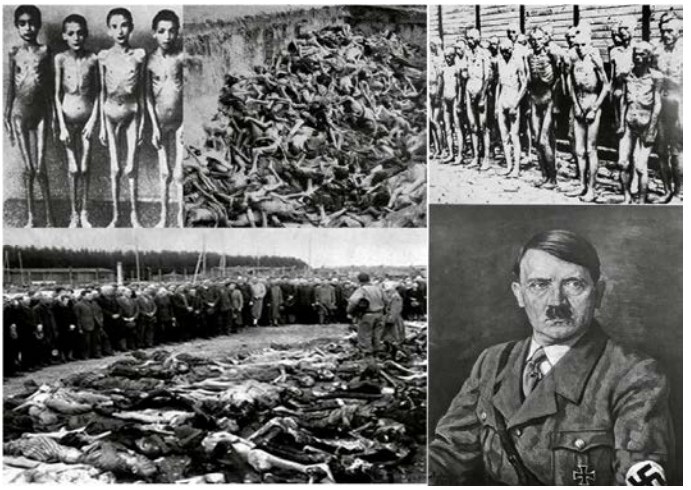


Figura 4. *Registros asociados con el holocausto provocado por el gobierno nazi*

Fuente: http://micuartosecret.blogspot.com/2015_01_01_archive.html

Se sumó a los hechos antes narrados de utilización de datos personales por parte del Estado para fines del aseguramiento de los intereses de las élites, circunstancias como las ocurridas durante el régimen

de extrema derecha establecido en España durante el gobierno del General Francisco Franco. En tal periodo, el seguimiento del gobierno sobre los registros fotográficos que se efectuaban en el territorio español, al igual que su autoría, constituían un registro de datos personales orientados al control de la divulgación de noticias contrarias al régimen, así como un mecanismo de identificación de agentes contrarios al mismo. Así lo estableció el bando promulgado el 11 de septiembre de 1936, como lo refiere Francisco Espinoza Maestre (Espinoza Maestre, 2005, p. 18), a raíz de la matanza de Badajoz – España, donde se ordenó que:

> Todo negativo, del que había que entregar una copia con los datos personales y del laboratorio impreso por detrás, tenía que pasar por censura previa… las casas de fotografías debían llevar un registro de todos los trabajos que realizaban y de todos los clientes, enviando copia de cada foto que revelaban a la División … entre los casos más sonados destaca el ocurrido a la Casa Kodak por revelar las imágenes que un cliente había tomado de los cadáveres que aparecían a diario en uno de los fusiladeros de la ciudad.

Figura 5. *Imágenes de la masacre de Badajoz, España, bajo el régimen de Francisco Franco, 1936*

Fuente: //www.publico.es/espana/76-anos-despues-matanza-badajoz.html

Las dolorosas realidades produjeron que los defensores de ideales democráticos e inspiradores de un nuevo pensamiento jurídico, com-

prendieran claramente la necesidad de incorporar en sus agendas temáticas el reclamo por el reconocimiento del valor superior de la dignidad humana, pero, de contera también la creación de ciertos derechos subjetivos instrumentales que le permitieran a los individuos la protección efectiva de su propia dignidad. Este sentir que no se circunscribió a los escenarios académicos y de los cerrados círculos del pensamiento humanista, pronto arribó a los más importantes foros internacionales que se consolidaban en ese momento: el seno de la Organización de Estados Americanos y la Organización de las Naciones Unidas.

El 2 de mayo de 1948 en Bogotá, capital de la República de Colombia, al interior de la Novena Asamblea Internacional de los Estados Americanos, como lo narra Amaya Úbeda de Torres (Úbeda de Torres, 2006, p. 212), fue aprobada la Declaración Americana de los Derechos y Deberes del Hombre. Como nota paradójica de la historia, cabe reseñar que mientras se cumplía los preparativos de tan trascendental reunión, la que anticipaba desde América para el mundo un canto a la vida, el 9 de abril caía asesinado el líder político liberal colombiano Jorge Eliécer Gaitán, según algunos historiadores, por orden del régimen político de la época y al parecer con el respaldo de la Agencia Norteamericana de Inteligencia –CIA–. (http://www.semana.com/nacion/articulo/quien-mato-gaitan/44012-3).

Jorge Eliecer Gaitán era, al momento de su muerte, la cabeza visible de la oposición política al gobierno conservador de la época con claras opciones de sucesión política. A raíz de estos hechos, como lo narra Gustavo Cote Uribe, político, literato e historiador (Cote Uribe, 1981, pp. 71-101), se desencadenaron hechos violentos en todo el país, especialmente en Bogotá, posteriormente conocidos como el Bogotazo, constituyéndose este en uno más de los tantos episodios de violencia partidista que sufrió Colombia durante el siglo xx. Parte de estos conflictos fueron superados a raíz de los «Pactos de Sitges y Benidorm» que dieron origen al Frente Nacional, un periodo de 16 años de alternación de poder entre los partidos Liberal y Conservador que permitieron apaciguar la violencia partidista, pero no obstante, exacerbaron una nueva violencia ideologizada, entre otras razones, por el cierre de los espacios de participación a fuerzas políticas diferentes a las tradicionales que suscribieron los pactos, conflicto aún hoy vigente, con más de 50 años y en trámite de negociación en las conversaciones de La Habana, Cuba.

En tanto, la incorporación del principio de dignidad en la DADH trajo consigo la incorporación al universo jurídico americano de nuevos mecanismos dirigidos a hacer efectiva la proclama. Uno de ellos, base inicial del posterior derecho a la protección de datos, lo constituyó el Derecho a la Intimidad. Este derecho fue establecido en el artículo 5.º, señalando 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.» De igual manera en el artículo 9.º, estableciendo que «Toda persona tiene el derecho a la inviolabilidad de su domicilio.» Y finalmente, en su artículo 10.º, señalando que «Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia.»

Meses más tarde a la aprobación de la DADH, el frío invierno del 10 de diciembre de 1948, no impidió a los representantes de los países miembros de la Organización de las Naciones Unidas que se dieron cita en aquella asamblea, cumplir a cabalidad su histórico papel en defensa de la dignidad humana, a partir de ese instante, reconocida ya con pretensiones de globalidad. La adopción de la Declaración Universal de los Derechos Humanos –DUDH–, en general y de manera muy especial el reconocimiento del derecho a la intimidad, abrieron el sendero por el cual habría de transitar hacia el universo jurídico, años más tarde, el derecho a la protección de datos personales en casi todos los países democráticos del mundo. Desde aquel día, el tema fue incorporado en la agenda internacional de las naciones democráticas. La simiente germinada fue plasmada en el artículo 12 de la DUDH así:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Se trató pues de reconocer una esfera de la existencia humana considerada como esencial y necesaria para el cabal y adecuado desarrollo del individuo. Un ámbito del individuo que pudiera mantenerse fuera, tanto de las injerencias morbosas de los particulares, como de las infiltraciones peligrosas de los Estados. Esta concepción jurídica recogía de manera precisa la dimensión de la privacidad, tan claramente descrita en el diccionario de la Real Academia de la Lengua Española que la define como el «Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión» [Real Academia

Española, Diccionario de la Lengua Española (DRAE), 2012]. El domicilio, las correspondencias, la vida privada de los individuos, constituyeron en principio los objetos de cubrimiento de estas nuevas disposiciones que posteriormente se expandieron hasta la particularidad ya no de la órbita de protección sino de los elementos contenidos o asociados a ellos, esto es por ejemplo, la dirección del domicilio o los números telefónicos, los contenidos de los mensajes o de la correspondencia, las actividades desarrolladas al interior de la vida familiar (gustos, orientaciones sexuales, etc.) que, constituyendo las singularidades del individuo, a la postre terminaron siendo datos personales cuya protección debía ser asegurada.

3.2 LA DIÁSPORA JURÍDICA

El proceso de desarrollo del tema de protección de datos, como todos los institutos jurídicos, no ha sido ni concomitante ni homogéneo en todas las latitudes jurídicas. Sin embargo, visto el instituto desde una perspectiva universal, es posible identificar ciertos momentos claramente marcados en la historia de su evolución. Así es como, apoyados en el trabajo desarrollado por Ahti Saarenpää, profesor de Derecho Privado y director del Instituto de Leyes e Informática de la Facultad de Leyes de la Universidad de Lapland en Finlandia (Saarenpää, 2003, pp. 15-29), es posible hablar de cinco momentos de apariciones normativas así:

3.2.1 PERIODO PRE-DIGNIDAD

Con ello se quiere referenciar aquel periodo ocurrido hasta antes de la aparición en 1948 de las Declaraciones Universal de los Derechos Humanos –DUDH– y Americana de los Derechos del Hombre –DADH–, instrumentos estos que, como quedó advertido, incorporaron la noción de dignidad universal con propósito globalizante, por primera vez en la historia, y sembraron las bases dogmáticas de los desarrollos que habrían por venir en materia de protección de datos. Durante este periodo no se registra ningún tipo de reglamentación específica sobre protección de datos personales, circunstancia explicable entre otras en la carencia de una noción de dignidad universal consolidada.

No pueda pasarse por alto, durante este periodo, la aparición de las Declaraciones de Independencia de Estados Unidos de América de 1776 y de los Derechos del Hombre y del Ciudadano de 1789 en París, instrumentos ambos que constituyeron puntos de quiebre frente a modelos feudales y de seguro el más sólido escalón en el difícil ascenso del humanismo jurídico. No obstante también hay que reconocer que una y otra, aún estaban lejos de incorporar la trascendente noción de dignidad que en las declaraciones posteriores se desarrolló. Como nota curiosa que pone de relieve lo afirmado, se resalta que en los 17 artículos de la proclama francesa de 1789 la única referencia a la dignidad, se hace en el artículo 6 utilizándose el término de forma sinónima a cargo o empleo. Y tanto en la americana como en la francesa, nunca hay referencia alguna a los antecedentes de la protección de datos personales como lo son la intimidad y el buen nombre.

IN CONGRESS, JULY 4, 1776.

A DECLARATION

BY THE REPRESENTATIVES OF THE

UNITED STATES OF AMERICA,

IN GENERAL CONGRESS ASSEMBLED.

WHEN in the Courſe of human Events, it becomes neceſſary for one People to diſſolve the Political Bands which have connected them with another, and to aſſume among the Powers of the Earth, the ſeparate and equal Station to which the Laws of Nature and of Nature's God entitle them, a decent Reſpect to the Opinions of Mankind requires that they ſhould declare the cauſes which impel them to the Separation.

We hold theſe Truths to be ſelf-evident, that all Men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among theſe are Life, Liberty, and the Purſuit of Happineſs.--That to ſecure theſe Rights, Governments are inſtituted among Men, deriving their juſt Powers from the Conſent of the Governed, that whenever any Form of Government becomes deſtructive of theſe Ends, it is the Right of the People to alter or to abolish it, and to inſtitute new Government, laying its Foundation on ſuch Principles, and organizing its Powers in ſuch Form, as to them ſhall ſeem moſt likely to effect their Safety and Happineſs. Prudence, indeed, will dictate that Governments long eſtabliſhed ſhould not be changed for light and tranſient Cauſes; and accordingly all Experience hath ſhewn, that Mankind are more diſpoſed to ſuffer, while Evils are ſufferable, than to right themſelves by abolishing the Forms to which they are accuſtomed. But when a long Train of Abuſes and Uſurpations, purſuing invariably the ſame Object, evinces a Deſign to reduce them under abſolute Deſpotiſm, it is their Right, it is their Duty, to throw off ſuch Government, and to provide new Guards for their future Security. Such has been the patient Sufferance of theſe Colonies; and ſuch is now the Neceſſity which conſtrains them to alter their former Syſtems of Government. The Hiſtory of the preſent King of Great-Britain is a Hiſtory of repeated Injuries and Uſurpations, all having in direct Object the Eſtabliſhment of an abſolute Tyranny over theſe States. To prove this, let Facts be ſubmitted to a candid World.

He has refuſed his Aſſent to Laws, the moſt wholeſome and neceſſary for the public Good.

He has forbidden his Governors to paſs Laws of immediate and preſſing Importance, unleſs ſuſpended in their Operation till his Aſſent ſhould be obtained; and when ſo ſuſpended, he has utterly neglected to attend to them.

He has refuſed to paſs other Laws for the Accommodation of large Diſtricts of People, unleſs thoſe People would relinquiſh the Right of Repreſentation in

Figura 6. *Declaración Americana de Independencia de 1776*

Fuente://www.biografiasyvidas.com/monografia/washington/fotos4.htm

Finaliza este periodo con los acontecimientos dolorosos de la segunda guerra mundial, la puesta en evidencia de las atrocidades cometidas por regímenes de extrema derecha y la necesidad de realizar pactos globales entre las naciones para evitar la repetición de lo ocurrido.

3.2.2 PERIODO DE FUNDAMENTACIÓN HUMANISTA

Se denomina así en virtud de la unificación ideológica de grandes bloques nacionales en torno, por primera vez en la historia, al reco-

nocimiento de la dignidad como un principio universal como respuesta a las experiencias vividas con ocasión de, en ese momento, la recientemente finalizada segunda guerra mundial (abril de 1945). Su hito fundante lo constituyen la DUDH y la DADH en 1948 y abarca un amplio periodo hasta antes de la aparición de la Ley de Protección de Datos Personales del Land Hesse en Alemania en 1970 y la primera Ley de Suecia de 1973.

Figura 7. *La Presidenta de la Comisión de Derechos Humanos, señora Eleanor Roosevelt, leyendo la Declaración Universal de Derechos Humanos en español*

Fuente: //www.un.org/es/events/humanrightsday/2008/photos.shtml

Debe destacarse que durante este periodo se da la incorporación, en la gran mayoría de las Constituciones del mundo democrático, del principio superior de la dignidad y el derecho a la privacidad, aunque la consolidación de la normativa en materia de derecho a la protección de datos personales habría de tener que esperarse hasta el año de 1970.

Otro acontecimiento que sería de trascendencia para el desarrollo ulterior de las normativas en materia de protección de datos personales fue la conformación del Consejo de Europa –CE–. Inicialmente Bélgica, Francia, Luxemburgo, Países Bajos y Reino Unido suscribieron el 5 de mayo de 1949 la Carta fundacional a la cual posteriormente adhirieron Irlanda, Italia, Dinamarca, Noruega y Suecia, y

> Una de las primeras medidas de la recién creada organización fue la redacción en 1950 (Roma 4 de noviembre) del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

> Este texto recogía en un instrumento jurídico de obligado cumplimiento los derechos enunciados dos años antes por la Declaración Universal de Derechos Humanos. En 1953 entró en vigor y desde entonces ha sido una pieza clave en la actuación de la entidad (Ministerio de Asuntos Exteriores y Cooperación, 1949).

Tal como lo refiere Lucrecio Rebollo Delgado (Rebollo Delgado, 2014, p. 140), este convenio consagró

> (…) una serie de derechos y libertades civiles y políticas, y por otra establece un sistema dirigido a garantizar el respeto por parte de los Estados contratantes, de las obligaciones por ellos asumidas. Tres instituciones se repartían esta responsabilidad de control: la Comisión Europea de Derechos Humanos (establecida en 1954), el Tribunal Europeo de Derechos Humanos (instituido en 1959) y el Comité de Ministros del Consejo de Europa, compuesto por los ministros de Asuntos Exteriores de los Estados miembros o sus representantes.

El artículo 8 de la Convención, en concordancia con la DUDH, como se precisa en sus considerandos, consagró el reconocimiento del derecho al respeto de la vida privada y familiar en los siguientes términos:

> Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2 No podrá haber ingerencia (sic.) de la autoridad pública en el ejercicio de este derecho salvo cuando esta ingerencia (sic.) esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de terceros.

Cabe resaltarse que, en este momento de la historia, las nuevas tecnologías de las comunicaciones y las advertencias normativas de protección a la intimidad, empiezan a producir las primeras manifestaciones. Por ejemplo, con miras a lograr la integración europea y advirtiendo los retos que traerán los desarrollos tecnológicos frente a la información personal, en 1967 se constituyó la Comisión Consultiva de la Comunidad Europea del Carbón y del Acero, organismo al cual se encomendó que, como lo refiere Ofelia Tejerina Rodríguez (Tejerina Rodrígue, 2014, p. 72), estudiaría,

> (…) la potencial agresividad de la tecnología sobre los derechos de los individuos, y que elaboró el dictamen que informaría la Resolución 509 de la Asamblea del Consejo de Europa sobre derechos humanos y los nuevos logros científicos, de 1968, centrada principalmente en el análisis del derecho a no sufrir injerencias en la vida privada.

Este periodo se cierra momentos antes de la aparición de las primeras normas nacionales sobre protección de datos personales que vieron como pionera la muy reconocida Ley de Protección de datos del Estado Hesse en Alemania de 1970.

3.2.3 PERIODO DE INSULARIDAD NORMATIVA

Su nombre deriva del fenómeno ocurrido con ocasión de la aparición de legislaciones en materia de protección de datos personales al interior de cada una de las naciones, las que por tener en cada caso aspectos muy propios de sus culturas jurídicas locales, tendieron a generar circunstancias de entorpecimiento a las dinámicas comerciales transfronterizas como consecuencia de la intensión de protección de la data personal que incorporaban. Este periodo se ubica entre 1970, fecha de aparición de la ley de Protección de Datos Personales del Land Hessen, Alemania, hasta antes del Convenio del Consejo de Europa 108 del 28 de enero de 1980 sobre Datos Personales.

El hito lo constituye sin lugar a dudas, como se ha afirmado, la ley del Estado de Hesse. Sobre ella señala Alberto Cerda Silva (Cerda Silva, 2003) que:

> (…) en 1970 se promulga la Datenschutz, ley sobre tratamiento de datos personales del Land de Hesse, en la República Federal de Alemania, mediante la cual se pretendía brindar protección a las personas naturales ante la amenaza que representaba el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del Estado, los municipios y entidades locales rurales, así como las demás personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal. A efectos de asegurar el cumplimiento de sus previsiones, la ley creaba el Comisario de Protección de Datos, al cual garantizaba independencia para el desempeño de sus funciones, cuales eran velar por la observancia de los preceptos de la propia ley y cuantos otros hicieren referencia al trato de los datos de los ciudadanos.

La finalidad que esta ley perseguía, al igual que algunas otras de su generación, la constituía fundamentalmente proteger a los individuos frente a las injerencias que pudiera ejecutarse con ocasión de la utilización de las nuevas tecnologías. Ello refleja la estrecha relación existente, para la época, entre el derecho a la intimidad y la protección de los datos personales, fase inicial de surgimiento de este derecho.

Esta Ley de Hesse constituyó el antecedente de la *Bundesdatenschutzgesetz* o Ley Federal de Protección de Datos de la República Federal Alemana de 1977 (Cerda Silva, 2003, pp. 45-75). La nueva norma fue modificada años más tarde (1990) por la ley «de perfeccionamiento (Fortentwicklung) de elaboración de datos y protección de datos». En esta última, la descripción de la finalidad denota un avance significativo en la conceptualización del derecho a la protección de datos personales, toda vez que, tal como se lee en la Sección 1.ª, sobre Disposiciones Generales, numeral 1, el objeto de la misma ahora será «…proteger al individuo contra la lesión que en su derecho a la personalidad causare el trato (Umgang) con sus datos personales» (Manuel Heredero, p. 1768), expresión que pone de presente la dimensión autónoma que en ese momento empieza a dársele al derecho de protección de datos personales. Obsérvese que hasta antes de esta nueva norma, el núcleo de amparo perseguido lo constituía la intimidad, se buscaba entonces proteger al individuo de la trasgresión de su esfera personal por parte terceros no autorizados que pudieran actuar apoyados con los nuevos mecanismos tecnológicos.

Con esta nueva disposición, el núcleo de amparo normativo se desplaza de la intimidad, a los datos mismos en función de la autodeterminación informática y la responsabilidad por el autorizado en función de ella a tratar los datos de otro. Es por ello que no se requerirá la evidencia del daño afectado por la trasgresión de la intimidad, sino que bastará para imputar responsabilidad, el simple inadecuado manejo que de los datos se realice en contravía a lo reglado por las nacientes disposiciones. A partir de ese instante, podrá sancionarse por el solo hecho de no cumplir con los mecanismos de seguridad en la protección de los datos personales de alguien que autoriza su recolección, así no se hubiere violado la esfera de la intimidad de aquel.

Dentro de otras normativas surgidas durante este periodo, cabe destacar la Data Lag 289 de 1973 en Suecia que, como lo reseñan Sánchez Pérez y Rojas González (Sánchez Pérez & Rojas González, 2012), junto con la referida del Estado Hesse, es «una de las primeras leyes de protección de datos en el mundo». Esta también pionera normativa, como lo reseña Alberto Cerda Silva (Cerda Siva, 2006),

> (…) imponía un sistema de registro abierto para publicitar los bancos de datos personales relativo a personas físicas realizado por medios automatizados, los que debían ser previamente autorizados para funcionar, asociado a una autoridad de control –la Datainspektionen, expresión del

> Ombudsman proyectado al tratamiento de datos– que vela por el respeto de la ley, con facultades inspectoras, normativas y procesales para requerir la aplicación judicial de sanciones.

Posteriormente vinieron otras normas como la *Privacy Act* de 1974 en Estados Unidos, con la cual se pretendió garantizar tres derechos a saber:

1. Consulta de bases de datos sobre sí mismo *(The right to see records about oneself),* 2. Rectificación del dato *(The right to request the amendment of records that are not accurate, relevant, timely or complete),* y 3. Derecho a la protección de la intimidad frente a la recolección, almacenamiento y divulgación de información personal *(The right of individuals to be protected against unwarranted invasion of their privacy resulting from the collection, maintenance, use, and disclosure of personal information)* (Congreso de los Estado Unidos, 1974).

Le siguieron a esta norma, en Dinamarca, las leyes sobre ficheros públicos y privados de 1978, en Austria la Ley Federal de Protección de Datos de 1978 y entrada en vigencia el 1 de enero de 1980 *(Bundesgesetz vom 18 Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz –DSG–),* la Ley 78 de enero 17 de 1978 en Francia que reguló lo relativo a la información, las bases de datos y las libertades, entre otras leyes y, finalmente, en el plano de la Unión Europea, durante este periodo surgen la Resolución 22 de 1973 sobre la protección de la privacidad de los individuos de cara a la banca electrónica en el sector privado, la Resolución 29 de 1974 sobre la protección de los individuos de cara a los datos electrónicos en la banca pública y la Resolución del Parlamento Europeo del 8 de mayo de 1979 «sobre tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática» (Tejerina Rodríguez, 2014, p. 73).

Como puede observarse, este fue un periodo prolífero en materia de expedición de leyes de protección de datos personales en el mundo europeo y en Norteamérica particularmente. No obstante, esta multiplicidad de legislaciones nacionales y federales, si bien poseían en común los principios inspiradores, por otra parte, como se dijo, debido a sus particulares características causantes de asimetrías normativas, se convirtieron en limitantes de la comunicación comercial transfronteriza en momentos en que la misma se consolidaba como consecuen-

cia de la globalización afincada en los avances de las nuevas tecnologías. Esta dificultad fue puesta de presente justamente, entre otras, por la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 1980) al punto que, en la Introducción del Memorándum Explicativo de las Directrices Relativas a la Protección de la Intimidad y de la Circulación Transfronteriza de Datos Personales del 23 de septiembre de 1980, advirtió que:

> Una particularidad de los países miembro de la OCDE en el último decenio ha sido la elaboración de leyes para la protección de la intimidad, las cuales propenden a asumir diferentes formas en distintos países, y en muchos de ellos están todavía en vías de elaboración. Las disparidades en la legislación pueden crear obstáculos a la libre circulación de información entre los países. Tal circulación se ha incrementado en gran medida en los últimos años y seguramente seguirán creciendo a resultas de la introducción de nueva tecnología informática y de comunicaciones.

Justamente este documento de la OCDE invitaba a la búsqueda de una legislación común a los Estados miembros del tratado, con miras a superar los riesgos de aislacionismo informático y económico.

3.2.4 PERIODO DE UNIFICACIÓN EUROPEA

Como su nombre mismo lo indica y a consecuencia de las circunstancias anotadas anteriormente sobre multiplicidad de normas nacionales, este periodo se caracteriza por un esfuerzo muy significativo al interior de la Unión Europea por lograr la unificación normativa de tratamiento de los datos personales. Abarca desde el Convenio 108 sobre Datos Personales del Consejo de Europa de 1980 hasta 1995 con la aprobación de la Directiva 95/46/CE, de octubre 24, del Parlamento Europeo y del Consejo, sobre Protección de las Personas Físicas en lo referido al «tratamiento de datos personales y a la libre circulación de estos datos», inclusive.

Tal como proféticamente lo había advertido George Catlett Marshall (Marshall, 1947) en su histórico discurso pronunciado en la Universidad Harvard el 5 de julio de 1947 y a partir del cual se estableciera el plan de recuperación económica de la Europa de post guerra denominado posteriormente Plan Marshall, la única manera en que podría superarse no solo la devastación física (vías, puentes, edificios, comunicaciones, colegios, hospitales, etc.) y moral (una gran pérdida de confianza en sí mismos) sino por sobre todo la devastación de la eco-

nomía de los países europeos (antiguas industrias pujantes ahora rezagos de fábricas armamentistas, bancos quebrados, aseguradoras desvertebradas, la confianza resquebrajaba, etc.) era mediante un esfuerzo nacido de la propia Europa que involucrara la voluntad de sus naciones por unificar sus esfuerzos en el propósito común de su nuevo desarrollo. Así fue como, a raíz de las palabras del General Marshall, en el marco de las aterradoras circunstancias de devastación y gracias a la afortunada concurrencia de naciones, el 16 de abril de 1948 se dio origen a la Organización para la Cooperación Económica Europea, conocida por sus siglas en inglés como OEEC, antecedente institucional de la Organización para la Cooperación y el Desarrollo Económico –OCDE–, transformada en tal a partir de 1961, organismo que en este periodo «de unificación europea» vino a cumplir un rol trascendente en la generación de normativa de protección de datos personales, entre otras, labor en que se ocupa aún hoy día. Prueba de esto último lo constituye la reciente declaración del Secretario General Ángel José Gurría (Gurría, 2015) de dicha institución que, refiriéndose a Colombia y su proceso de preparación para ingresar a partir de 2016 a la OCDE, señalaba que:

> En este caso estamos en una mecánica distinta a la que opera para quienes ya son miembros. Esta consiste en llevarlos a que sean miembros plenos. Eso quiere decir mucho trabajo con los distintos comités, alineando reglamentos, leyes, códigos. Eso se hace una sola vez, claro. Pero en la parte sustantiva, lo que hacemos es apoyar las reformas colombianas.

De hecho, los intentos de unificación normativa europea en materia de protección de datos personales se terminan desarrollando en este periodo en la línea de las denominadas Recomendaciones de la OCDE de 1980. La similitud de dichas recomendaciones con el Convenio 108 del Consejo de Europa son evidentes, entre otras explicable en razón a la participación de similares integrantes en los equipos redactores.

Pero las recomendaciones del Convenio 108 requerían de una disposición con fuerza vinculante. Por ello, luego de enormes esfuerzos para lograr la unificación normativa, finalmente llega, a través de la Directiva 95/46/CE del 24 de octubre, la norma europea de protección de datos.

Respecto de la dimensión jurídica de las Directivas que genera el Consejo, la Comisión o el Parlamento Europeo, como lo consagra el documento «Diálogo con los ciudadanos y las empresas - Protección

de datos en la Unión Europea» (Oficina de Publicaciones Oficiales de las Comunidades Europeas, 2000), resulta oportuno recordar que:

> Una directiva es una norma legislativa europea destinada a los Estados miembros. Una vez adoptada a escala europea, cada Estado miembro debe garantizar su aplicación efectiva en su sistema jurídico. La directiva dispone el resultado final. La forma y los métodos de aplicación corren a cargo de cada Estado miembro. En principio, una directiva entra en vigor mediante las medidas nacionales de aplicación (legislación nacional). No obstante, cabe la posibilidad de que, aunque un Estado miembro no haya aplicado una directiva, parte de lo dispuesto en ella pueda tener efectos directos. Esto significa que si una directiva confiere derechos directos a las personas físicas, estas podrán alegar ante un juez tal directiva sin tener que esperar su aplicación en la legislación nacional. Además, si las personas físicas opinan que se han visto perjudicadas por una incorrecta aplicación de la directiva por parte de las autoridades nacionales, tendrán derecho a denunciarlas por daños y perjuicios. Esto solo podrá hacerse ante tribunales nacionales.

La Directiva 95/46, proferida por el Parlamento Europeo y el Consejo de la Unión Europea, puesta en vigencia como la carta de navegación en materia de «protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos», se publicó en el Diario Oficial n.° L 281 de 23/11/1995 p. 0031-0050.

Dentro de las consideraciones que constituyeron razón para la aprobación de la Directiva 95/46 (Unión Europea, 1995, p. Considerado 2), estuvieron, entre otras, el reconocimiento de una realidad económico-tecnológica como es el incremento, todos los días mayor, de los intercambios comerciales de los países miembros de la Unión Europea generadores inexorables de flujo transfronterizos de datos personales soportados en tecnologías de la información y las comunicaciones, las diferencias normativas entre dichos países que impedían los procesos de intercambio y la necesidad de unificarlas para generar seguridad jurídica, así como, obviamente, la obligatoria necesidad de proteger a las personas humanas, por considerar que

> Los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar –contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos (Unión Europea, 1995, p. Considerado 2).

Entre algunos aspectos a destacar de la Directiva 95/46 CE pudiere referenciarse los siguientes:

Su principal causa generadora la constituye la necesidad de la unificación normativa, de donde se deriva un fin tanto de facilitación de intercambio interno y transfronterizo de datos como la protección de las personas en virtud del tratamiento de los mismos.

Sobre el tema del régimen de responsabilidad por el tratamiento de datos personales es muy importante señalar que la Directiva pareciera proponer un sistema objetivo de responsabilidad al afirmar en su Consideración 55 que:

> (…) los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos, el cual solo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor (Unión Europea, 1995, p. Considerado 2).

Establece como principios del tratamiento de datos los de autodeterminación informática, legalidad, finalidad, integralidad, confidencialidad, seguridad, información, entre otros, así como el establecimiento de los derechos de acceso, rectificación, oposición de los titulares.

Crea la categoría especial de datos para referir con ello a los que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, pertenencia a sindicatos, de salud y sexualidad.

Quizá uno de los aspectos más relevantes de la Directiva 95/46 CE es haber constituido la base para la creación de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD), norma que ha marcado un derrotero fundamental en el periodo siguiente como quiera que se constituirá en el referente para América Latina y base del trasplante normativo que motiva el presente trabajo.

Con posterioridad a la expedición de la Directiva 95/46 CE, le siguió, como era de esperarse en virtud de la tendencia de integración internacional jalonada por la OECD, un proceso de llegada de las normas europeas a otras latitudes como la latinoamericana, abriendo el camino a una nuevo periodo de desarrollo normativo.

3.2.5 PERIODO DE TRASPLANTE NORMATIVO

Corresponde al último periodo de desarrollo normativo de datos personales. Se identifica como comprendido en el lapso que inicia después de la aparición de la Directiva 95/46/CE y llega hasta los presentes días. Está caracterizado por la aparición de normas en el universo jurídico nacional de los países en vía de desarrollo que recogen contenidos, tanto de las manifestaciones unificadas de la experiencia europea, como de las recomendaciones de la OCDE, cuando no directamente leyes como la LOPD española.

Se denomina «de trasplante normativo», para poner en evidencia, en términos de Diego López Medina (López Medina, 2012), que lo ocurrido no es cosa diferente a un intento condicionado por las dependencias macroeconómicas, de incorporar, no siempre de manera exitosa, el conocimiento generado en el núcleo, principalmente proveniente de países como Alemania, Inglaterra, Estados Unidos o España.

Este fenómeno de trasplante normativo en general se ha visto acelerado por la acción de los organismos internacionales (Banco Mundial, Fondo Monetario Internacional o la OCDE) que, en ejercicio de su posición dominante sobre los países de la periferia, buscan consolidar la nueva fase de globalización económica caracterizada justamente por la unificación normativa. Constituyen ejemplo de esto las recientemente incorporadas en el ámbito latinoamericano normas de protección al consumidor, las normas de regulación contable conforme a los estándares internacionales de información financiera (NIIF) o de contabilidad para el sector público (NICSP), solo para citar algunos ejemplos.

Los efectos de este trasplante normativo, en materia de datos personales, se registró tempranamente en América Latina al interior de aquellos países que llegaron primero a establecer relaciones con la OCDE, como lo fueron Chile y Argentina. Hoy, transcurrida más de una década, el tema se ha extendido a varios ordenamientos jurídicos de la región que, cuando no en leyes especiales que regulan el tema, han incorporado por lo menos mandatos constitucionales sobre protección de datos, algunos de los cuales están a la espera de sus correspondientes desarrollos legislativos.

Como ilustración de lo afirmado se referencian algunos países del continente sur:

— *Chile*. Constitución Política artículo 19 numeral 4. Ley 19628 de del 28 de agosto de 1999 de «Sobre Protección de la Vida Privada, con modificaciones el 13 de junio de 2002 por Ley 20463, el 22 de julio de 2011 por Ley 20521 y el 17 de febrero de 2012 por la Ley 20575. (http://www.leychile.cl/Navegar?idNorma=141599)

— *Argentina*. Constitución Nacional art. 43 párrafo 3.º, Ley 25.326 de octubre 4 de 2000 de Protección de Datos Personales, Decreto Reglamentario 1558 del 29 de noviembre de 2001. (http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm)

— *México*. La Ley Federal de Protección de Datos Personales en Posesión de Particulares» del 5 de julio de 2010, entró en vigor un día después y tiene efecto a partir de enero del año 2012.» (http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010)

— *Costa Rica*. Constitución Política art. 24. Ley 8968 de. 5 de septiembre de 2011 de «Protección de la persona frente al Tratamiento de sus datos personales», Decreto Ejecutivo 37.554 – JP del 5 de marzo de 2013. (http://www.tse.go.cr/pdf/normativa/leydeproteccion delapersona.pdf)

— *Perú*. Constitución Política art. 2.º numerales 6 y 7. La Ley 29.733 del 2 de julio de 2011 de «Protección de datos personales», Decreto Supremo No 003-2013-JUS de (http://www. educacionenred.pe/noticia/?portada=8167).

— *Guatemala*. Constitución Política artículos 24 y 30. Proyecto legislativo No. 4090-2009 de Protección de Datos Personales. No se identificó aún su aprobación. (http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn_guatemala.asp)

— *Brasil*. Lei n.º 12.965 de abril 23 de 2014 o Marco Civil de Internet, que regula los «Principios, Garantías, Derechos y Deberes para el uso de Internet en Brasil». Como lo indica su propio título, no es una ley de protección de datos personales, aun cuando incorpora algunas disposiciones como la inviolabilidad del acceso o las comunicaciones vía internet. Justamente en el año 2015 se ha iniciado una discusión pública sobre el proyecto de ley de protección de datos específicamente, respecto del cual el periodista Pedro Ozores comenta que «Mientras algunos creen que la iniciativa representa los tentácu-

los regulatorios del Estado para extenderse más allá de la vida de la gente, otros piensan que el proyecto es esencial para definir la manera en que los datos de los ciudadanos deben manejarse. El Ministerio de Justicia argumenta que Brasil está atrasado pues leyes similares han entrado ya en vigor en más de 100 países. En América Latina, por ejemplo, Chile analiza una actualización de su propia legislación» (Ozores, 2015). (http://www.harmonywithnatureun.org/content/documents/159Bolivia%20Consitucion.pdf)

— *Ecuador.* Constitución artículo 92. Consagra la acción de Hábeas Data. No obstante se identificó la ley de protección de datos personales. (http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf)

— *Bolivia*. Constitución Política del Estado Plurinacional artículos 25, 130 y siguientes. Consagra la acción de protección de privacidad. No obstante se identificó existencia de ley de protección de datos personales. (http://www.harmonywithnatureun.org/content/documents/159Bolivia%20Consitucion.pdf)

Como se aprecia, la expansión del reciente pensamiento en materia de protección de datos personales no se hizo esperar. Habiendo surgido como ideal democrático, pasando a proclama universal, finalmente llegó a convertirse en instituto jurídico en diferentes Estados.

Colombia, que no ha sido la excepción, por ser el objeto central del presente trabajo, será abordado en el siguiente capítulo, en tanto, puede afirmarse, con base en las anotaciones planteadas, que el instituto del Derecho a la Protección de Datos Personales, en menos de 60 años, pasó de ser una mera referencia en las prácticas sociales y empresariales a tener una entidad jurídica propia y cada vez más compleja. Su crecimiento vertiginoso ha estado directamente ligado a los desarrollos tecnológicos, sobre todo de las comunicaciones. El tema de los datos personales se encuentra asociado prácticamente a todos los escenarios de la vida cotidiana, generando una tensión permanente entre privacidad e información, que tiende a incrementarse con la llegada primero del internet en las redes, luego el internet de las cosas (ropa con microchips, electrodomésticos inteligentes, Smartphone con gps, pasaportes con dispositivos incorporados, etc.) y ahora el más recientemente y desafiante desarrollo tecnológico con el que podría denominarse el internet de las personas a través de los denominados dispositivos RFID (Radio Frequency Identification), en español

identificación por radiofrecuencia, de utilización subcutánea que entre otras desató una enorme polémica en los Estados Unidos de Norteamérica, pues opositores del gobierno del presidente Obama, le imputaron, a raíz de la ley de salud por él aprobada en el Congreso, implementar como obligatorio este dispositivo por mandato de la denominada Ley Obamacare a partir del año 2013, circunstancia que a la postre resultó falsa, pero no por ella improbable.

Hoy el tema fácilmente nos recuerda las vivencias de Winston, personaje de la novela de George Orwell (Orwell, 1984) del «Gran Hermano, a quien describe en la siguiente escena:

> Winston tenía que subir a un séptimo piso. Con sus treinta y nueve años y una úlcera de varices por encima del tobillo derecho, subió lentamente, descansando varias veces. Encada descansillo, frente a la puerta del ascensor, el cartelón del enorme rostro miraba desde el muro. Era uno de esos dibujos realizados de tal manera que los ojos le siguen a uno adondequiera que esté. EL GRAN HERMANO TE VIGILA, decían las palabras al pie.

Los días de la incipiente protección de datos personales como una dimensión del derecho a la intimidad, quedaron atrás. El nuevo ecosistema jurídico que ha generado la protección de datos es tan grande y complejo, como inmensas e intrincadas son las relaciones sociales y económicas en esta era de las redes virtuales. El reto que se le impone ahora a los nuevos desarrollos del instituto jurídico, es por sobre todo, ponderar con justicia la administración de la tensión que siempre estará detrás del tema de la protección de datos personales: por una parte, la necesidad de garantizar la libre empresa, hoy un requerimiento de mayor exigencia en la nueva fase del capitalismo global, y, por la otra, la necesidad de la protección del ser humano en su dignidad, en esta nueva era del constitucionalismo basado en la protección de los derechos fundamentales, máxime cuando la asimetría entre las corporaciones globales y el individuo, es todos los días mayor.

Peter Hustinx, Supervisor Europeo de Protección de Datos (Hustinx, 2014) en el Resumen ejecutivo del dictamen preliminar sobre Intimidad y competitividad en la era de la obtención de datos masivos, dejó planteada la tensión señalada en los siguientes términos:

> El mercado o mercados en línea en rápida expansión […] afectan cada vez más a todos los aspectos de los negocios. Asegurarse de que la competencia funciona de manera efectiva en estos mercados será una de las

> principales prioridades […] la creciente recopilación, tratamiento y uso de datos de las transacciones de los consumidores con fines comerciales... está resultando ser una fuente de ventajas competitivas cada vez más importante [que podría convertirse en], una creciente fuente de perjuicios para el consumidor.

4. HÁBEAS DATA EN COLOMBIA

4.1 MARCO SOCIO POLÍTICO DE SURGIMIENTO DEL HÁBEAS DATA

La Constitución Política de Colombia que rigió hasta el año de 1991, que como ya se ha afirmado en apartes anteriores no consagraba expresamente el principio de dignidad universal aunque sí normas que amparaban este presupuesto, lejos estaba de llegar a incorporar el derecho a la autodeterminación informática y con él el derecho a la protección de datos personales.

Lo más aproximado al tema, normativamente hablando, lo constituía el artículo 23 de la derogada norma superior que consagraba el derecho a la intimidad en los siguientes términos:

> nadie podrá ser molestado en su persona o familia, ni reducido a prisión o arresto, ni detenido, ni su domicilio registrado, sino a virtud de mandamiento escrito de autoridad competente, con las formalidades legales y por motivo previamente definido en las leyes.

A lo consagrado en esta disposición se le adicionaba la protección de las comunicaciones consagrada en el artículo 38 que advertía:

> La correspondencia confiada a los telégrafos y correos es inviolable. Las cartas y papeles privados no podrán ser interceptados ni registrados sino por la autoridad, mediante orden de funcionario competente, en los casos y con las formalidades que establezca la ley y con el único objeto de buscar pruebas judiciales.

Es decir que, en términos de «arqueología jurídica», estas disposiciones constituyen algunos de los registros ancestrales del moderno concepto de la protección de datos personales.

La aparición de la protección de datos personales en materia constitucional solo llegaría a Colombia en el año de 1991, momentos en los cuales, conforme al cronograma universal de la Protección de Datos Personales, transcurría el denominado «Periodo de Consolidación Europea» (quepa recordar que 11 años atrás, en 1.980 se había ya aprobado el Convenio 108 sobre Datos Personales del Consejo de Europa y que faltarían solo cuatro años para el alumbramiento, en el año 1995, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo), circunstancia que entre otras pone de manifiesto la tardía aparición de estos temas en el concierto nacional.

Este año 1991, sin duda, fue histórico para la vida institucional de la República, pues se incorporaron quizá, considerando los últimos 100 años, los mayores cambios estructurales en el ordenamiento jurídico nacional. Sin embargo el contexto en que surgieron estos, y de contera el derecho a la protección de datos, estuvo precedido de circunstancias dolorosas que bien resultan pertinentes recrear para la mejor comprensión de lo ocurrido y de la interpretación sociológica de las normas surgidas.

Horacio Serpa Uribe (Serpa Uribe, 2009), ex presidente de la Asamblea Nacional Constituyente, describe de esta forma el precedente histórico y político de lo acaecido:

> En la época de los años 80, del siglo pasado, el país estaba asediado por la guerrilla, el paramilitarismo, el narcotráfico, la corrupción y la desigualdad. El narcotráfico había llegado a su máxima expresión de violencia y entre las miles de víctimas que había cobrado figuran los aspirantes a la Presidencia de la República doctores Jaime Pardo Leal, Luis Carlos Galán Sarmiento, Bernardo Jaramillo y Caros Pizarro León-Gómez. La comunidad reclamaba soluciones y convivencia. Los estudiantes, estremecidos por la violencia y afectados por el asesinato de Galán, recogieron con entusiasmo, compromiso y beligerancia la propuesta de convocar a una Asamblea Constituyente. No lo permitía la arcaica legislación vigente por entonces. Finalmente, sorteados toda clase de inconvenientes y talanqueras, fue aprobada plebiscitariamente durante el gobierno del doctor Virgilio Barco, el mismo día en que se eligió como sucesor al doctor César Gaviria Trujillo. El 9 de diciembre de 1990 fueron elegidos popularmente 70 Constituyentes. Dos más, con plenos derechos, fueron designados por el Presidente de la República para que representaran al desmovilizado Ejército Popular de Liberación –E. P. L.– y otros dos, con voz pero sin voto, representaron a los grupos ex guerrilleros Quintín Lame y Partido Revolucionario de los Trabajadores –P. T. R.–, según autorización legal expedida para lograr acuerdos de paz con los sectores subversivos. El 5 de febrero de 1991 comenzó a deliberar la Gran Asamblea bajo la copresidencia de Álvaro Gómez Hurtado, Antonio Navarro Wolf y Horacio Serpa Uribe. El 4 de julio del mismo año se expidió la nueva Carta Fundamental.

La Asamblea Nacional Constituyente de 1991 dio a la luz de la juridicidad nacional una carta de navegación signada por innovadores conceptos filosóficos de humanismo y principios ideológicos de sentido social, que reivindicaron la dignidad del ser humano como titular de derechos fundamentales, proclamando responsabilidades de género no reconocidas antes, alertando del compromiso irredento con la infancia y cantando una proclama épica al reconocimiento de una realidad multiétnica y pluricultural históricamente negada hasta

ese instante. No obstante, hay que señalar que esta misma carta constitucional, con claros acentos sociales, constituyó la llave que abrió la senda de los ajustes nacionales a la globalización que trajo la apertura económica y con ella los efectos del relanzamiento del nuevo modelo de acumulación de capital, esta vez mucho más agresivo. Para ello, a diferencia de lo ocurrido en otros lugares del mundo, el país no estaba preparado, razón por la cual se produjo una profunda afectación a los incipientes desarrollos industriales, sobre todos asociados al agro, quienes sucumbieron ante la mayor competitividad de los agentes económicos extranjeros, estos mucho mejor preparados, cuando no subvencionados por los mismos Estados que le exigieron a Colombia acogerse al nuevo modelo «no intervencionista».

Y es justamente en el marco de esas realidades de la historia nacional, muchas de ellas dolorosas, que el Hábeas Data llega al país por vía de su incorporación en el artículo 15 de la nueva Constitución Política, reglándose, a su tenor, en los siguientes términos:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
>
> La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.
>
> Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Pero no obstante la novedad de la figura constitucional del Hábeas Data referida, en gracia de la verdad, hay que reconocer que este derecho a la protección de datos ya había asomado algunas manifestaciones en el universo jurídico nacional antes del advenimiento de la nueva carta superior. Esto se evidencia, entre otras, en contenidos como el de la Ley 23 de 1981 «Por la cual se dictan normas en materia de ética médica», que en su artículo 34 dispuso que la Historia Clínica «… Es un documento privado, sometido a reserva, que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley».

En igual sentido lo había registrado también la Ley 96 de 1985 que, incorporando disposiciones sobre el régimen electoral, en su artículo 51, habiendo considerado como públicos los datos contenidos en el Registro Civil de las personas y referido a

> … el número, lugar y fecha de expedición de documentos de identidad pertenecientes a terceros», le señaló carácter de reservado a «… las informaciones que reposen en los archivos de la Registraduría, referentes a la identidad de las personas, cómo son sus datos biográficos, su filiación y fórmula dactiloscópica.

Respecto de esta última norma cabe advertirse que a primera vista pareciera haber sido derogada con la Ley 1266 de 2008 en razón a que su artículo 3, literal f, señaló como públicos los datos «relativos al estado civil de las personas», expresión repetida posteriormente en el decreto 1074 de 2015 artículo 2.2.2.25.1.3 numeral 2, reglamentario de la Ley 1581 de 2012. En opinión de quien desarrolla el presente trabajo, por la especificada de la materia al igual que el ámbito de aplicación de la Ley 1266 de 2008, no puede entenderse como derogada por ella la ley 96 de 1985. Mucho menos podrá afirmarse de parte del Decreto 1377 de 2013, el cual, por su rango en la estructura jerárquica normativa colombiana, no tiene vocación de derogatoria de ley, máxime cuando las expresiones del Decreto no reflejan el contenido normativo de la ley reglamentada esto es la Ley 1581 de 2012 (LEPD). De ello se concluye que, el artículo 51 de la Ley 96 de 1985 continúa vigente, debiéndose llamar la atención sobre tal circunstancia a todo el sistema de registro de Registro Civil (Registraduría del Estado Civil y Notarias), artículo que obviamente debe armonizarse con el Decreto Ley 1270 de 1970 que contiene el Estatuto del Registro Civil de la Personas.

4.2 MARCO REGULATORIO COLOMBIANO DEL HÁBEAS DATA

El marco regulatorio del Hábeas Data en Colombia se ha venido consolidando poco a poco a partir de la incorporación de su reconocimiento en la Constitución de 1991, en tres fases claramente identificadas. Por una parte un momento exclusivamente desarrollado por la jurisprudencia nacional, por sobre todo la surgida del órgano de cierre constitucional como lo es la Corte Constitucional. Posteriormente una segunda fase correspondiente a la aparición de normas especiales, esto

es la Ley 1266 de 2008 para información financiera, la que surge de la mano de normativa penal de los delitos informáticos consagrados en la Ley 1273 de 2009. Una tercera fase correspondiente al desarrollo de la normativa general de datos personales de personas naturales con la Ley 1581 de 2012 y finalmente, la fase que podría denominarse de reglamentación administrativa, en la cual se encuentra actualmente la temática, entre otras a la espera de la puesta en funcionamiento de todo el sistema de registro de bases de datos personales o registro de ficheros, tema ya avanzado desde hace un tiempo en España, que como se ha dicho constituye referente para estas latitudes.

A continuación se realiza una aproximación a los desarrollos alcanzados, con el propósito de permitir una visión panorámica del marco regulatorio colombiano sobre el Hábeas Data.

4.2.1 REGLAMENTACIÓN JURISPRUDENCIAL DEL HÁBEAS DATA. EL CAMINO HASTA LA AUTONOMÍA

El desarrollo del derecho de Hábeas Data en Colombia ha estado impulsado fundamentalmente desde la Corte Constitucional (órgano de cierre de la jurisdicción constitucional surgida de la nueva Constitución Política de 1991) resaltándose dentro de sus pronunciamientos la Sentencia SU-082 de 1995, que constituye precedente jurisprudencial y sentencia arquimédica tanto para el desarrollo ulterior de la jurisprudencia como para la línea legislativa que surgió posteriormente.

Por tal razón en el presente escrito se refieren el camino recorrido por la jurisprudencia constitucional colombiana desde el inicio del instituto jurídico hasta hoy en día, enmarcándolo en las tres grandes líneas que le han caracterizado, advirtiéndose de su existencia incluso concomitantemente en diversos momentos de la historia jurisprudencial nacional:

4.2.1.1 **Protección de datos personales como garantía del derecho a la intimidad**

Para iniciar, recuérdese que la protección de datos personales o Hábeas Data no siempre ha sido considerada como un derecho autó-

nomo. Sus primeras expresiones en el mundo jurídico se dieron como manifestación ínsita del derecho a la intimidad, al punto de ser considerada como un mecanismo de amparo o garantía de la misma. De esta circunstancia se derivaba que no se pregonara responsabilidad por uso indebido de datos personales si ello no había conllevado en sí misma una transgresión a la intimidad o al buen nombre del sujeto a quien se vinculaba los datos.

Cabe recordar que, para el inicio del instituto del Hábeas Data, el derecho a la intimidad se definía en los siguientes términos:

> La Constitución reconoce a toda persona el derecho fundamental a la intimidad personal y familiar (CP art. 15), antes protegida por la inviolabilidad del domicilio y la correspondencia. La finalidad principal de este derecho es resguardar un ámbito de vida privada personal y familiar, excluido del conocimiento ajeno y de cualquier tipo de intromisiones de otros, sin el consentimiento de su titular. El núcleo esencial del derecho a la intimidad define un espacio intangible, inmune a intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ver lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto (Sentencia T- 530 de 1992).

Con base en tal criterio conceptual la Corte Constitucional, por ejemplo, cuando resolvía asuntos relacionados con datos personales de contenido financiero reportado a centrales de riesgos en conflicto con el derecho a la información, los abordaba en perspectiva del derecho a la intimidad, tal como se evidencia en la SU-528 de 1993 que expresó:

> En casos de conflicto entre ambos, esta Sala no vacila en reconocer que la prevalencia del derecho a la intimidad sobre el derecho a la información, es consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial, a la vez, del Estado social de derecho en que se ha transformado hoy Colombia, por virtud de lo dispuesto en el artículo primero de la Carta de 1991 (…) Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de «personas virtuales» que afecten negativamente a sus titulares, vale decir, a las personas reales.

Para este momento, los conflictos sobre datos personales de carácter financiero eran fundamentalmente un conflicto a resolverse desde la perspectiva jurídica del derecho a la intimidad.

Estas primeras manifestaciones del Hábeas Data lo reconocían más como un mecanismo de «protección reforzada de la Intimidad». Sirve como ejemplo de lo advertido lo expresado por la misma Corte Constitucional en la Sentencia T-437 de 2004, cuando advierte:

> La intimidad ha sido reconocida por la Constitución como un derecho de carácter fundamental en el artículo 15. En esa disposición, el constituyente dispuso que «todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar». En esa misma norma, la Carta previó una protección reforzada de la intimidad, en aquellos casos en los cuales está de por medio (i) el conocimiento, actualización y rectificación de informaciones recogidas en bancos de datos y en archivos de entidades públicas y privadas, (ii) la correspondencia y (iii) los libros de contabilidad y demás documentos privados, de los que eventualmente podrá exigirse su presentación para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado.

4.2.1.2 **Protección de datos personales como manifestación del libre desarrollo de la personalidad**

Otra línea de pensamiento ha sido la expresada en la *Sentencia C-748 de 2011*, donde la Corte Constitucional reconoció que desde un inicio, al interior de sus miembros surgieron otras tendencias interpretativas como aquella que

> (...) consideraba el Hábeas Data una manifestación del libre desarrollo de la personalidad. Según esta línea, el Hábeas Data tiene su fundamento último (…) en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad.

Esta línea de pensamiento independientemente considerada, no ha tenido un gran desarrollo, sin embargo, hay que reconocer sí que alimentó las últimas tendencias del pensamiento jurisprudencial al aportar claridad en un componente del Hábeas Data como la dimensión de la autodeterminación informática.

4.2.1.3 **Protección de datos personales como derecho autónomo**

El reconocimiento del Hábeas Data como derecho autónomo no es de reciente aparición. Su existencia ha estado concomitantemente existiendo con las líneas anteriormente señaladas.

Para poner de manifiesto lo afirmado cabe leer la *Sentencia T-094 de 1995*, donde la Corte Constitucional definió *el Hábeas Data* como el

> (…) derecho autónomo y fundamental plasmado en el artículo 15 de la Constitución, que permite a toda persona conocer, actualizar y rectificar las informaciones que sobre ella hayan sido consignadas en bancos de datos y en archivos de entidades públicas o privadas, en defensa de sus derechos fundamentales a la intimidad, a la honra y al buen nombre.

En sentencias posteriores, poco a poco, se reafirmó esta línea conceptual, tal como, en palabras de la misma Corte Constitucional, se expresó:

> (…) a partir de la sentencia T-552/97, la jurisprudencia de la Corte deslindó como dos derechos autónomos estos dos conceptos, para concluir entonces que el artículo 15 de la Carta consagra en su texto tres derechos constitucionales diferenciados: el derecho a la intimidad, el derecho al buen nombre, y el derecho al Hábeas Data (Sentencia C-640 de 2010).

Se señaló en esta oportunidad que la Corte Constitucional*:*

> … reconoce que cuando la información recopilada no es veraz, actual o completa, el sujeto afectado puede invocar en su favor el Hábeas Data, garantía de índole procesal que le permite iniciar las acciones tendientes a obtener el conocimiento, la rectificación y actualización por parte de las entidades públicas o privadas a las que previamente autoriza manejar sus referencias comerciales. Tal fue el sentido de las providencias SU-082/95 y T-176/95 que establecieron lo siguiente: El contenido del Hábeas Data se manifiesta por tres facultades concretas (…): (a) El derecho a conocer las informaciones que a [las personas] se refieren; (b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; (c) El derecho a rectificar las informaciones que no correspondan a la verdad (Sentencia SU-082/95 M. P. Dr. Jorge Arango Mejía).

Posteriormente la Corte Constitucional, en la SU-458 de 2012, ratificó tal posición afirmando que:

> Como derecho autónomo, tiene el Hábeas Data un objeto protegido concreto: el poder de control que el titular de la información puede ejercer sobre quién (y cómo) administra la información que le concierne. En este sentido el Hábeas Data en su dimensión subjetiva faculta al sujeto concernido a conocer, actualizar, rectificar, autorizar, incluir, excluir, etc., su información personal cuando esta es objeto de administración en una base de datos. A su vez, como garantía, tiene el Hábeas Data la función específica de proteger, mediante la vigilancia del cumplimiento de las reglas y principios de la administración de datos, los derechos y libertades que dependen de (o que pueden ser afectados por) una administración de datos personales deficiente.

Esta última línea conceptual que reafirma la autonomía del derecho de Hábeas Data, y que no descarta ni se opone a la consideración de su labor de garantía de otros derechos como la intimidad o el buen nombre (como lo ha advertido la Corte Constitucional desde la Sentencia T-729 de 2002, ratificada en la SU-458 de 2012), constituye la base argumentativa para considerar como eventos de posible imputación de responsabilidad a quien actúa como Responsable o Encargado de datos personales (persona natural o jurídica) por el solo hecho de tratar los datos personales sin la incorporación de las «medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012» (artículo 2.2.2.25.6.1 del Decreto 1074 de 2015), aun cuando su comportamiento no hubiera trasgredido el buen nombre o la intimidad del titular o titulares de los datos. Así ocurre, por ejemplo, con las sanciones que pudiera imponer la Superintendencia de Industria y Comercio cuando identifican que sobre los datos sensibles no se han establecido los mecanismos tecnológicos necesarios para salvaguardar la seguridad de aquellos, *v. gr*. controles de acceso a bases de datos, mecanismos de cifrado de datos sensibles, circulación de datos sensibles por canales dedicados, etc.

Esta rápida vista panorámica que se describió sobre las tres líneas gruesas que han caracterizado el pensamiento jurisprudencial de la Corte Constitucional sobre la naturaleza del Hábeas Data en Colombia, permite concluir que, aun cuando la línea actualmente consolidada es la última expresada, esto es considerar el Hábeas Data como un derecho autónomo, ello no excluye, jurisprudencialmente hablando, su íntima relación con el derecho a la intimidad e incluso al buen nombre, pues sin lugar a dudas es un instrumento de protección de aquellos. Por otra parte no se está lejos de considerarse el Hábeas Data también como manifestación del libre desarrollo de la personalidad pues, como todos los derechos, está en la órbita de la voluntad del titular su ejercicio o no, por sobre todo en la dimensión que corresponde a la autodeterminación informática.

En resumen, las tres líneas que marcaron en principio el pensamiento jurisprudencial sobre Hábeas Data como tendencias independientes unas de otras, hoy se entrelazan re-conceptualizando este derecho como un derecho autónomo, instrumental y estrechamente relacionado con el libre desarrollo de la personalidad.

4.2.2 REGLAMENTACIÓN DEL HÁBEAS DATA FINANCIERO (LEY 1266 DE 2008)

Las líneas trazadas por la jurisprudencia Constitucional produjeron que, años más tarde, el Congreso de la República, por iniciativa del senador del Partido Liberal Luis Fernando Velasco (coordinador de ponentes de la ley 1581 de 2012), expidiera la Ley 1266 de 2008 sobre Hábeas Data, que luego el Gobierno Nacional reglamentó a través de los Decretos 1727 de 2009, 2952 de 2010 y 4886 de 2011. Al tenor de su mismo texto, la ley definió su objeto como:

> Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política (artículo 1 de la Ley 1266 de 2008).

El ámbito de regulación estuvo determinado «particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países» (artículo 1 de la Ley 1266 de 2008) referida a personas naturales y jurídicas, constituyéndose por tal razón en una disposición de carácter especial, asimilada en el ambiente nacional como Ley de Hábeas Data Financiero. Esta circunstancia produjo en el contexto social la errónea creencia de considerar que la misma solo era aplicable a las centrales de riesgo y a las entidades del sector financiero, perdiendo de vista que el artículo 3.º ibídem advertía que «se entenderá por información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen»(Subrayado fuera de texto). En tal sentido, todas aquellas entidades, públicas o privadas que, con ocasión de sus actividades, reporten a operadores de información (centrales de riesgos) datos de personas naturales o jurídicas, los operadores mismos y de igual manera quienes accedan a través de ellas en calidad de usuarios a dicha información quedan sometidos a las disposiciones contenidas en dicha ley, tal como lo ordenan entre otras los artículos 7.º, 8.º y 9.º de la Ley 1266 de 2008 al señalarles a cada uno obligaciones particulares en relación con los datos. Así por ejemplo un almacén de venta de electrodomésticos, ropa o cualquier otro artículo que, en razón a

otorgar crédito a sus clientes, reporte a las centrales de riesgo o las consulte para efectos de la concesión de estos, queda bajo el régimen de dicha ley.

En la siguiente figura se esquematiza el ámbito de las operaciones que se subsumen en el marco normativo de la referida ley.

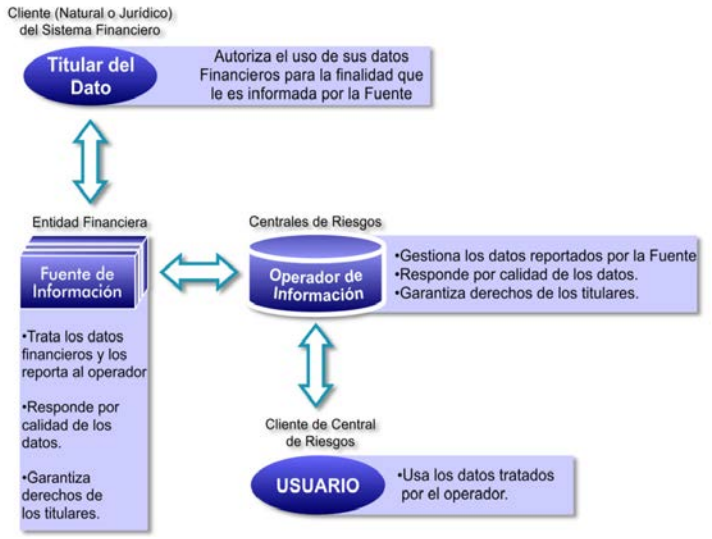


Figura 8. *Ámbito de regulación de la Ley 1266 de 2008*

«Los actores del sistema regulado por el Hábeas Data en general, deben operar conforme al principio de legalidad, esto es ajustados al ordenamiento que regula el tratamiento de datos personales.»

4.2.3 REGLAMENTACIÓN DEL HÁBEAS DATA PENAL (LEY 1273 DE 2009)

En el año siguiente a la expedición de la Ley 1266 del 2008, ahora con el propósito de prevenir y sancionar la afectación a la privacidad, la confiabilidad, la integralidad y la disponibilidad de la información en general y de los datos tratados en el marco del naciente régimen jurídico del Hábeas Data en particular, el legislador impregnado de los efectos globales causados por la preocupación sobre el tema y acogiendo las directrices jurídicas internacionales, incorporó al orde-

namiento penal la Ley 1273 de 2009 por medio de la cual «se crea un nuevo bien jurídico tutelado –denominado «de la protección de la información y de los datos»– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones» integrando, entre otros, los siguientes tipos penales directamente aplicables, entre otras, a la defensa de los principios asociados a la protección de datos.

4.2.3.1 Delitos asociados a la protección del principio de confidencialidad

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

4.2.3.2 Delitos asociados a la protección de los principios de disponibilidad, veracidad y completitud del dato

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

4.2.3.3 Delitos asociados a protección del principio de finalidad

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

La preocupación por la punibilidad de comportamientos que ponen en riesgo la privacidad de los datos personales en particular y de la información en general, se ha visto todos los días más agudizada al interior de los Estados, entre otras, para la imperativa necesidad de contrarrestar la labor emprendida por organizaciones dedicadas a realizar, con fines políticos, la denominadas *Fugas Éticas,* entendiendo por tales, en palabras de Kirk Hanson y Jerry Ceppos (Hanson & Ceppos, 2006):

> La divulgación de la información que expande la comprensión pública de un tema de interés público –sin dañar a nadie–. Una fuga también puede

> ser buena si ilumina la comprensión de un tema importante, aún si perjudica a alguien, siempre que el interés público en juego sea la vida y la salud cuando están en riesgo; un crimen, como el fraude cuando se está cometiendo; o si se trata de dineros públicos que están siendo malgastados.

Tal ha sido el caso de Wikileaks y su más visible miembro Julián Assange, asilado en la embajada de Ecuador en Londres desde el 19 de junio de 2012. Esta comunidad virtual por ejemplo, explica su acción de filtración ética afirmando:

> Nosotros somos partidarios de que hay que mantener un comportamiento ético en todas las circunstancias. Cada persona es el último juez de lo que es justo en su propia conciencia. Allí donde hay falta de libertad y donde la injusticia está anclada en la ley, hay lugar desde un punto de vista ético para la desobediencia civil. Allí donde el simple hecho de distribuir información pueda contribuir a poner en un aprieto a un régimen autoritario o a poner en evidencia un crimen, nosotros reconocemos el derecho, e incluso el deber, de llevarlo a cabo. Tales denuncias de irregularidades conllevan normalmente ciertos riesgos personales. Así, de la misma manera que hay en algunas jurisdicciones leyes que protegen a aquellos que denuncian irregularidades, Wikileaks proporciona medios y oportunidades para minimizar esos riesgos. Nosotros nos proponemos que todo gobierno autoritario, toda institución opresiva y todo gobierno corrupto sea objeto de presión, y no solo a través de la diplomacia internacional y de la libertad de información, o de las elecciones cada cuatro años, sino también a través de algo más poderoso: la propia conciencia individual de la gente que forma parte de ellos (WikiLeaks, 2007).

Constituye otro ejemplo el caso de «Anonymus», grupo que, al parecer, luego de haber surgido como un foro de discusión de *comics* japonesas (conocido inicialmente como *4chan),* desde el año 2008 se ha convertido en referencia para diferentes comunidades virtuales en el mundo, dedicadas a similares acciones como las desarrolladas por WikiLeaks. Justamente el 15 de noviembre de 2013, el hacker del grupo «Anonymous» Jeremy Hammond, considerado por el FBI como miembro de grupos terroristas *(The Guardian,* 2015), fue condenado a diez años de prisión y tres de libertad vigilada en Estados Unidos, «por haber filtrado 5 millones de correos electrónicos de la empresa de inteligencia y seguridad Stratford».

A la preocupación por reprimir penalmente las acciones asociadas a la violación de información y de contera a los datos personales, se ha sumado la lucha contra el «terrorismo», ahora exacerbada con ocasión de la aparición del denominado *Estado Islámico* y su lucha *Yihadista*. Tal es por ejemplo el caso español con las recientes normativas

adoptadas (modificaciones al Código Penal, la nueva Ley Antiterrorista y la Ley de Seguridad Ciudadana), las que de seguro llegarán al ordenamiento colombiano dada la alta influencia que dicha legislación está teniendo en el contexto latinoamericano. En estas nuevas disposiciones se califica de actos terroristas a lo que en el pasado era considerado delito informático, prendiendo las alarmas sobre el constante conflicto entre intimidad y seguridad. Las reacciones sobre el tema no se han hecho esperar. Por ejemplo, Xataka (Xataka, 2015), espacio web especializado en temas de internet, expresaba, a propósito de los nuevos delitos incorporados en el sistema Español, que «Se aprobaban definitivamente en el Congreso tres reformas de ley ampliamente criticadas por la oposición y también por otros grupos defensores de los derechos humanos (…)» y comentó algunos de los cambios surgidos de las normas, en referencia particular a ellos, así:

> **Amplia definición de «terrorismo»**: Entre otras cosas, se pasan a considerar los delitos informáticos como acciones terroristas si su objetivo es desestabilizar, alterar la paz pública o provocar estado de terror. Por ejemplo, atacar la web de un Ministerio será ahora un atentado terrorista. «Se considerarán igualmente delitos de terrorismo los **delitos informáticos** tipificados en los artículos 197 bis y 197 ter y 264 a 264 cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior».
>
> **Cuidado con lo que visitas:** «Acceder de manera habitual» a páginas web con contenidos dirigidos o «idóneos» para terroristas supondrá de dos a cinco años de cárcel, aunque no se especifica qué es «habitual» y de qué sitios web estamos hablando concretamente. «Se entenderá que comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines. Los hechos se entenderán cometidos en España cuando se acceda a los contenidos desde el territorio español.
>
> **Vigila a quién prestas tus servicios:** El prestar servicios tecnológicos se considera colaborar con los terroristas. «Será castigado con las penas de prisión de cinco a diez años y multa de dieciocho a veinticuatro meses el que lleve a cabo, recabe o facilite cualquier acto de colaboración con las actividades o las finalidades de una organización, grupo o elemento terrorista, o para cometer cualquiera de los delitos comprendidos en este capítulo. En particular son actos de colaboración la información o vigilancia de personas [...], la prestación de servicios tecnológicos, y cualquier otra forma equivalente de cooperación o ayuda a las actividades de las organizaciones o grupos terroristas, grupos o personas a que se refiere el párrafo anterior».

> **Bloqueo de contenidos:** El juez podrá ordenar a cualquier prestador de servicios (alojamiento, buscadores, etc.) que eliminen los enlaces a contenidos ilícitos relacionados con el terrorismo. «Si los hechos se hubieran cometido a través de servicios o contenidos accesibles a través de Internet o de servicios de comunicaciones electrónicas, el Juez o Tribunal podrá ordenar la retirada de los contenidos o servicios ilícitos. Subsidiariamente, podrá ordenar a los prestadores de servicios de alojamiento que retiren los contenidos ilícitos, a los motores de búsqueda que supriman los enlaces que apunten a ellos y a los proveedores de servicios de comunicaciones electrónicas que impidan el acceso a los contenidos o servicios ilícitos siempre que concurra alguno de los siguientes supuestos: (a) Cuando la medida resulte proporcionada a la gravedad de los hechos y a la relevancia de la información y necesaria para evitar su difusión. (b) Cuando se difundan exclusiva o preponderantemente los contenidos a los que se refieren los apartados anteriores.

El tema que gravita en el espacio de la punibilidad de comportamientos asociados al uso de la información, pone de relieve la tensión que muchas veces se refiere en este trabajo entre confidencialidad de la información (entre otras de los datos personales) y por tanto la privacidad, frente al derecho colectivo de estar bien y oportunamente informado. Los conflictos surgidos de esta tensión hasta ahora inician, pero sirve como antesala de lo que se vendrá en los próximos años, el caso del periodista español Jaime Alekos quien, entre otras, se ha dedicado a registrar, en medio de la crisis económica vivida en ese país, los desahucios que se practican para el cobro de obligaciones del sector financiero. El referido periodista el 3 de marzo de 2015 fue detenido e imputado de los delitos de «desobediencia, resistencia y atentado a agentes de la autoridad» (Alekos, 2015) justamente en razón a estar cubriendo el desalojo de la familia Gracia González en el Distrito Tetuán en la calle Ofelia Nieto 29 de la ciudad de Madrid.

Esta problemática relación de conflictividad se puede apreciar en su verdadera dimensión al leer las palabras del Dr. David P. Stewart (Stewart, 2012), miembro del Comité Jurídico Interamericano (CJI), cuando, en la «Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas» presentada en el 80.º período ordinario de sesiones de la OEA, celebrado en México D. F. entre el 5 y el 19 de marzo de 2012, advertía:

> Es evidente que el tema es dinámico, la discusión se mantiene activa, y los enfoques tanto nacionales como regionales siguen evolucionando. Cuáles prácticas específicas son aceptables y cuáles se deben circunscribir o prohibir muy probablemente dependerá de la manera en que se aborde

el problema. Las respuestas pueden diferir si se consideran desde la perspectiva de la seguridad nacional o de la aplicación de las leyes, o como asunto de reglamentación social, o desde la perspectiva de proteger la innovación tecnológica, promover el comercio y el desarrollo, proteger contra intrusiones del extranjero, etc. Por el momento es necesario concluir que no existe una «talla única». Un intento de describir o imponer un solo enfoque normativo detallado tiene pocas probabilidades de lograr aprobación amplia a corto plazo.

4.2.4 REGLAMENTACIÓN DEL HÁBEAS DATA DE PERSONAS NATURALES (LEY 1581 DE 2012)

Avanzadas las líneas del pensamiento jurisprudencial, aparecida la Ley especial de Hábeas Data en temas financieros y puesto en funcionamiento el estatuto penal de delitos informáticos, finalmente, de suyo en forma tardía, el Congreso de la República expidió la Ley 1581 de 2012, reconocida como Ley de Protección de Datos.

En la siguiente figura se esquematiza el ámbito de las operaciones que se subsumen en el marco normativo de la referida ley.

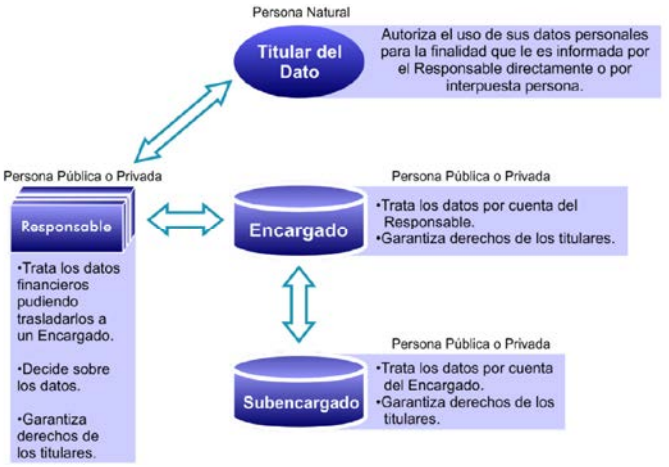


Figura 9. *Ámbito de regulación de la Ley 1581 de 2012*

«La ley 1581 de 2012, norma general de Hábeas Data, define los actores sometidos al sistema regulatorio, conceptos que deben aplicarse en concordancia con las normas especiales del Hábeas Data Financiero, cuando la relación involucre eventos regulados por este.»

Esta norma que constituye norma de carácter general, fue reglamentada por el Gobierno nacional a través de los Decretos 1377 de 2013 y 886 de 2014, recogidos textualmente en el Decreto 1074 del 26 de mayo de 2015 o Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Con base en estas disposiciones, la Superintendencia de Industria y Comercio –SIC–, además de poner en funcionamiento la Superintendencia delegada para la Protección de Datos Personales (a través de ella la SIC empieza a ejercer funciones en Colombia al estilo de la Agencia Española de Protección de Datos –AEPD–), el 28 de octubre de 2013, expidió la Circular Única que, entre otros apartes, en su Título V desarrolló el tema de «Protección de datos personales» dirigida a orientar el cumplimiento de obligaciones propias del Hábeas Data Financiero (Ley 1266 de 2008).

Al momento de la elaboración del presente trabajo, la SIC prepara la incorporación del segundo capítulo al mencionado Título V de la Circular Única, dirigido a orientar la inscripción de las bases de datos que tratan las entidades privadas (inspirado en el modelo español de inscripción de ficheros) tanto para datos asociados a Hábeas Data financieros como de Datos Personales (Ley 1581 de 2012). De esta manera, a la fecha, este es el estado del arte normativo de la protección de datos personales en Colombia, surgido en medio de una conflictividad que aún se espera, con fe, sea prontamente superada.

4.3 PRINCIPIOS RECTORES DEL HÁBEAS DATA

El ámbito en que se desarrolla el derecho de Hábeas Data y por tanto la órbita de regulación de todas las operaciones que los actores involucrados ejecutan cuando de datos personales se refiere, se encuentran sometidos al principio superior constitucional de Dignidad –PC–, pero adicionalmente a un conjunto de principios que, aun cuando algunos de ellos surgidos primigeniamente en la jurisprudencia, hoy poseen soporte legal motivo por el cual se clasifican como principios legales –PL– y, por otro lado, otros cuyo origen ha sido netamente jurisprudencial denominado por ello principios jurisprudenciales –PJ–, unos y otros en todo caso de obligatoriedad, tal como la jurisprudencia constitucional lo ha reconocido en diversas ocasiones, como por ejemplo las sentencias T-729 de 2002, C-185 de 2003, C-748 de 2011, C-1011 de 2008. Para una mejor comprensión y pos-

terior profundización del tema a lectores interesados, se citan a continuación con sus correspondientes referencias normativas y jurisprudenciales, así:

4.3.1 PRINCIPIO DE DIGNIDAD (PC)

Es el principio y valor superior por antonomasia del ordenamiento jurídico nacional, tal como quedó señalado en el primer aparte del presente capítulo. En virtud del mismo, toda acción u omisión asociada al tratamiento de datos personales debe ejecutarse siempre salvaguardando la dignidad del Titular y amparando concomitantemente los demás derechos constitucionales y en especial el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Cualquier comportamiento que violente este principio se entiende violatorio del ordenamiento superior, debiéndose proscribir por tanto toda actuación que así resulte calificada.

4.3.2 PRINCIPIO DE LEGALIDAD (PL)

Señala este principio que el tratamiento a que se refiere la Ley LEPD, «es una actividad reglada, debiéndose por tanto estar sometida a todas las disposiciones que le regulan» y a los principios que lo enmarcan (Ley 1581 de 2012).

4.3.3 PRINCIPIO DE LIBERTAD (PL)

Conforme a este principio:

> (...) los datos personales solo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos de manera ilícita (ya sea sin la previa autorización del titular o en ausencia de mandato legal o judicial). En este sentido por ejemplo, se encuentra prohibida su enajenación o cesión por cualquier tipo contractual. (Sentencia T-729 de 2002.)

Sobre este principio la Corte Constitucional advirtió en la SU-028 de 1995, que:

> (...) los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular. Obsérvese la referencia especial que la norma hace a la libertad, no solo económica sino en todos los órdenes. Por esto, con razón se ha dicho que la libertad, referida no solo al aspecto económico, hace parte del núcleo esencial del Hábeas Data.

En similar sentido se produjeron las sentencias T-022 de 1993, SU-082 de 1995 (consideraciones sexta y décima), T-097 de 1995, T-552 de 1997, T-527 de 2000 y T-578 de 2001, así como se refiere la Ley 1266 de 2008, en el párrafo 2 del parágrafo del artículo 6.º y la LEPD de 2012 artículo 4 literal c).

4.3.4 PRINCIPIO DE VERACIDAD O CALIDAD (PL)

Ordena el sentido de este principio que «los datos personales deben obedecer a situaciones reales, deben ser ciertos, de tal forma que se encuentra prohibida la administración de datos falsos o erróneos» (Sentencia T-729 de 2002), conforme a lo preceptuado en la Ley 1581 de 2012, artículo 4, literal d, que señaló: «La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible».

En similar sentido se pronunció la Corte Constitucional en las sentencias SU-082 de 1995 y SU-089 de 1995, T-097 de 1995, T-527 de 2000, T-578 de 2001, T-1085 de 2001, Ley 1266 de 2008, artículo 4, literal a).

4.3.5 PRINCIPIO DE INTEGRIDAD (PL)

La Ley 1266 de 2008, artículo 4, literal a. y Ley 1581 de 2012, artículo 4, literal d) lo consagran y como lo ha afirmado la Corte Constitucional, este principio está «estrechamente ligado al de veracidad» (T-729 de 2002). En virtud del mismo,

> (...) la información que se registre o se divulgue a partir del suministro de datos personales debe ser completa, de tal forma que se encuentra prohibido el registro y divulgación de datos parciales, incompletos o fraccionados. Con todo, salvo casos excepcionales, la integridad no significa que una única base de datos pueda compilar datos que, sin valerse de otras bases de datos, permitan realizar un perfil completo de las personas. (Sentencia T-729 de 2002.)

4.3.6 PRINCIPIO DE FINALIDAD (PL)

Este principio consagrado en la Ley 1266 de 2008, art. 4, literal b, y la Ley 1581 de 2012 art. 4, literal b), sin perjuicio de la importancia que los demás principios revisten, constituye base esencial para el tratamiento de datos personales, pues su establecimiento está dado en función de la exigencia de la autorización informada, según la cual no podrá recolectarse datos personales sin la autorización previa, expresa y debidamente informada, constituyendo esta última exigencia justamente la obligación que le asiste a Responsables y Encargados por señalarle al Titular la finalidad para la cual se captura el dato. En virtud de este principio,

> (...) tanto el acopio, el procesamiento y la divulgación de los datos personales, debe obedecer a una finalidad constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista. (Sentencia T-729 de 2002.)

Para mayor información pueden verse las siguientes sentencias C-1011 de 2008 y T-176A de 2014.

4.3.7 PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA (PL)

Este principio se encuentra

> (...) estrechamente ligado al de finalidad, la divulgación y circulación de la información está sometida a los límites específicos determinados por el objeto de la base de datos, por la autorización del titular y por el principio de finalidad, de tal forma que queda prohibida la divulgación indiscriminada de los datos personales. (Sentencia T-729 de 2002, M. P. Eduardo Montealegre Lynett. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm.)

En similar sentido se produjo la sentencia T-176A de 2014. Por otra parte, la Ley 1581 de 2012 en el artículo 4, literal f, adicionalmente advierte que igualmente constituyen límite del tratamiento de datos la naturaleza de estos.

Como consecuencia de este principio, los datos no pueden ser tratados por cualquier persona de la organización Responsable o Encar-

gada, pues solo podrán hacerlo quienes, en virtud de sus roles y competencias deban entrar en contacto con los datos.

4.3.8 PRINCIPIO DE TRANSPARENCIA (PL)

Según este principio los Responsables y Encargados deben estar en condiciones de suministrar al Titular, en cualquier momento, información «acerca de la existencia de los datos que le conciernen» tal como lo advierte la Ley 1581 de 2012, artículo 4, literal e). Respecto de este principio cabe anticipar que el rango de consulta que le asiste al Titular del Dato es bastante más amplio que simplemente indagar sobre la existencia de los mismos, tal como se aborda en el acápite del Titular del Derecho de Hábeas Data y sus Facultades en líneas adelante.

4.3.9 PRINCIPIO DE SEGURIDAD (PL)

El principio de seguridad implica la necesidad de instrumentar las medidas técnicas, humanas y administrativas que resulten requeridas para blindar los datos de adulteraciones, pérdidas y acceso no autorizado tal como se desprende de la Ley 1581 de 2012, artículo 4, literal g. La exigencia que mana de este principio obviamente debe entenderse acorde con la naturaleza de la organización, el tipo de dato tratado, el tamaño de la operación y de la organización, el riesgo creado a los Titulares, entre otros aspectos.

4.3.10 PRINCIPIO DE CONFIDENCIALIDAD (PL)

A partir de este principio quienes por razón de sus roles y competencias tengan acceso autorizado a datos personales, están en la obligación de no divulgarlos aún después de finalizada la relación que dio ocasión a ello, como lo ordena la Ley 1581 de 2012, artículo 4, literal h).

4.3.11 PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA (PL)

En virtud de este principio los Responsables o los Encargados, están en la obligación de poder demostrar ante los organismos de con-

trol (Superintendencia de Industria y Comercio o los jueces de la República) que han implementado adecuadamente las «medidas apropiadas y efectivas» para cumplir con las obligaciones establecidas en la Ley. Sobre este aspecto la autoridad de datos personales de Colombia, esto es la SIC, ha publicado la Guía de Implementación del Principio de Responsabilidad Demostrada o Accountability, conforme a la Ley 1581 de 2012 artículo 26 y su Decreto 1074 de 2015, que puede ser consultado en la página www.fersaco.com.

4.3.12 PRINCIPIO DE TEMPORALIDAD DE LA INFORMACIÓN (PL)

Por mandato de este principio «La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos» (Ley 1266 de 2008, artículo 4, literal d). Se advierte que por estar este principio íntimamente ligado a la caducidad del dato, se ha dedicado en capítulo posterior un aparte para abordar este aspecto en mayor dimensión.

4.3.13 PRINCIPIO DE INTERPRETACIÓN INTEGRAL DE DERECHOS CONSTITUCIONALES (PL)

En correlación con el principio de dignidad, este principio consagrado en la Ley 1266 de 2008, artículo 4, literal e), advierte que la aplicación de las leyes de Hábeas Data se interpretará:

> (...) en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables.

4.3.14 PRINCIPIO DE NECESIDAD (PJ)

Asociado al principio de finalidad y utilidad:

> los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y di-

> vulgación de datos que no guarden estrecha relación con el objetivo de la base de datos (T-729 de 2002 y T-176 de 1995).

En la sentencia T-307 de 1999 (consideración 20), la Corte Constitucional manifestó respecto de este principio que:

> la información solicitada por el banco de datos, debe ser la estrictamente necesaria y útil, para alcanzar la finalidad constitucional perseguida. Por ello, los datos solo pueden permanecer consignados en el archivo mientras se alcanzan los objetivos perseguidos. Una vez esto ocurra, deben desaparecer.

4.3.15 PRINCIPIO DE UTILIDAD (PJ)

Como se dijo, en concordancia con el principio de necesidad y finalidad, la utilidad del dato es aspecto a tenerse en cuenta por parte de los Responsables y Encargados. Es decir que al momento de definirse la finalidad para la cual se va a recolectar el mismo, debe de igual manera indagarse por quien así procede acerca de si el dato efectivamente resulta útil para el logro de la finalidad propuesta. En tal sentido la Corte manifestó:

> (...) tanto el acopio, el procesamiento y la divulgación de los datos personales, debe cumplir una función determinada, como expresión del ejercicio legítimo del derecho a la administración de los mismos; por ello, está prohibida la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara o determinable. (Sentencia T-729 de 2002.)

De manera similar se aprecia el pronunciamiento de la Corte Constitucional cuando afirmó que se debe:

> (...) cumplir una función determinada, acorde con el ejercicio legítimo de la administración de los datos personales. Por lo cual queda proscrita la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara y suficientemente determinable (T-176A de 2014 y en similar sentido C-1011 de 2008).

4.3.16 PRINCIPIO DE INCORPORACIÓN (PJ)

Proclama este principio que igual que en una base de datos se registran los datos negativos sobre un Titular, aquellos datos que resulten favorables a aquel deberán ser incorporadas igualmente. Por ejemplo en el evento de centrales de riesgos financieros donde se almacena como historia financiera el estado de mora de un deudor, ha

de registrarse también la información en el evento del pago de la misma. En tal sentido la Corte manifestó:

> (...) cuando de la inclusión de datos personales en determinadas bases, deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exija para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos. (Sentencia T-729 de 2002.)

4.3.17 PRINCIPIO DE CADUCIDAD (PJ)

Este principio, que ha de entenderse articuladamente con las anotaciones que sobre inhabilidades intemporales se tratará en capítulos adelante, proclama que

> la información desfavorable al titular debe ser retirada de las bases de datos siguiendo criterios de razonabilidad y oportunidad, de tal forma que queda prohibida la conservación indefinida de los datos después que han desaparecido las causas que justificaron su acopio y administración. (Sentencia T-729 de 2002.)

4.3.18 PRINCIPIO DE INDIVIDUALIDAD (PJ)

Finalmente, en virtud del principio de finalidad se prohíbe la minería de datos a partir de bases de datos recolectadas por fuentes y actividades diversas. La razón se explica en el principio de finalidad pues, al exigirse que la misma tenga que ser informada para efectos de la recolección del dato y de esta forma cumplir con la autorización informada, las nuevas bases de datos que surgen del ejercicio de minería suelen corresponder a nuevas finalidades que extralimitan por tanto el marco de la autorización inicial.

Al respecto la Corte manifestó:

> (...) las administradoras deben mantener separadamente las bases de datos que se encuentren bajo su administración, de tal forma que queda prohibida la conducta dirigida a facilitar cruce de datos a partir de la acumulación de informaciones provenientes de diferentes bases de datos. (Sentencia T-729 de 2002.)

4.4 ELEMENTOS INTEGRADORES DEL HÁBEAS DATA

Referenciado como ha quedado el marco socio político de surgimiento del Hábeas Data, el marco jurisprudencial colombiano, los

referentes legislativos y el marco de principios que lo regulan, es ahora necesario identificar los elementos que constituyen el Hábeas Data, para lo cual resulta necesario adentrarse en la norma general que lo regula, esto es la Ley 1581 de 2012, no obstante advirtiendo que se estará haciendo referencia a la norma especial del Hábeas Data Financiero contenido en la Ley 1266 de 2008 cuando ello resulte pertinente.

4.4.1 NÚCLEO ESENCIAL Y CONTENIDO ADYACENTE DEL DERECHO FUNDAMENTAL DE HÁBEAS DATA EN LA LEY 1581 DE 2012

Durante el desarrollo del presente trabajo, se ha venido haciendo referencia, en diferentes momentos, a Hábeas Data, Protección de Datos Personales y Autodeterminación Informática, según fuere necesario. Sin embargo se ha dejado, exprofeso, este acápite para señalar que estos tres términos que aun cuando describen aspectos diferentes, tal como la misma jurisprudencia nacional lo ha advertido soslayadamente, hacen referencia a un mismo instituto jurídico. Cual es pues el sentido de cada una, cual el contenido del derecho en referencia, que relación se da entre cada uno de ellos, son cuestiones que se abordan en los apartes subsiguientes, pero para lo cual se hace menester realizar algunas precisiones preliminares.

Así entonces se debe, en primer lugar, indicar que, gramaticalmente, la expresión Hábeas Data se encuentra conformada por dos palabras: Hábeas, de origen latín, «1. “habeô, ês, êre, habuî, habitum”: “tener”», y, Data, «1. “dô, as, are, dedî, datum”: “dar”» (Gobierno de España - Ministerio de Educación, 2015), que si bien en los orígenes se refería a cualquier cosa dada, con posterioridad quedó referida a hechos o información. De allí se puede definir entonces la expresión Hábeas Data como tener la información o el dato, es decir poner de presente el dato.

Hoy día, con la expresión Hábeas Data se hace referencia a un derecho que, entrañando a su vez una acción de origen constitucional de similar nombre, está dirigido a proteger los datos (singularidades del individuo como se advirtió en el capítulo primero de este trabajo) tanto de personas naturales como de las jurídicas.

Resulta claro entonces entender que Hábeas Data o derecho sobre los datos (como se considera más adecuada su denominación), corresponde al derecho constitucionalmente consagrado en el artículo 15 superior de la carta colombiana, cuya característica es la de ser un derecho fundamental, autónomo e instrumental y por tanto de aplicación directa. En virtud de este derecho, el Titular, persona natural o la jurídica, puede o no autorizar a un(os) tercero(s) el tratamiento de sus propias singularidades (datos personales) y exigirle, en el evento en que lo autorice, a tener un comportamiento adecuado a los principios y buenas prácticas de la gestión de la seguridad de los mismos.

De la definición anterior se deriva que el Derecho sobre los datos o Hábeas Data, implica una doble dimensión, esto es la Autodeterminación Informática por una parte y por la otra el Aseguramiento Informático o Protección de Datos Personales, los cuales constituyen el primer elemento del referido derecho, pues enmarcan la órbita de su comprensión.

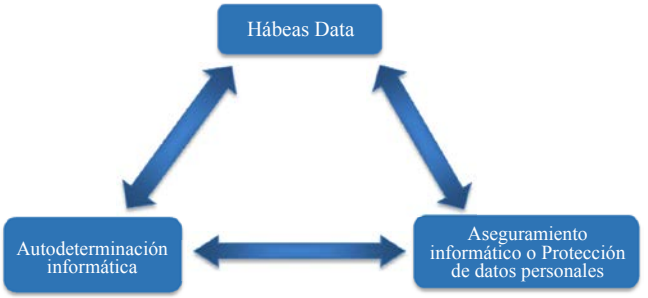


Figura 10. *Dimensiones del derecho subjetivo del Hábeas Data. Núcleo Esencial: autodeterminación informática*

«El Hábeas Data, en general, incorpora en el titular del derecho la doble facultad de definir a quien entrega los datos (autodeterminación informática) salvo orden legal o judicial y el derecho de exigir siempre, que sean tratados de forma segura (Aseguramiento informático de datos personales»

4.4.1.1 Núcleo Esencial: disponibilidad del dato

Esta primera dimensión se materializa en la posibilidad que tiene el titular del Hábeas Data para decidir a quien, en qué circunstancias,

con qué finalidad y de qué manera se autoriza el uso de sus propias singularidades (datos personales), por ejemplo: ADN, huella, voz, gustos, ideología, parentesco, creencias, orientaciones sexuales, etc. En términos de la jurisprudencia, la autodeterminación informática «faculta al sujeto concernido a conocer, actualizar, rectificar, autorizar, incluir, excluir, etc., su información personal cuando esta es objeto de administración en una base de datos» (SU-458 de 2012).

Esta dimensión del Hábeas Data constituye el núcleo, también llamado en algunas ocasiones como contenido mínimo del derecho, elementos estructurales esenciales (así por ejemplo la sentencia C-646 de 2001) o contenido básico, en los términos señalados por la Jurisprudencia que al respecto ha señalado, apoyada en la Teoría del Núcleo Esencial, que

> los derechos fundamentales tienen: (i) un núcleo o contenido básico que no puede ser limitado por las mayorías políticas ni desconocido en ningún caso, ni siquiera cuando un derecho fundamental colisiona con otro de la misma naturaleza o con otro principio constitucional… (Sentencia C-748 de 2011.)

Esto explica el por qué la Ley 1581 de 2012 es una ley estatutaria, como quiera que

> De conformidad con la jurisprudencia constitucional es competencia del legislador estatutario desarrollar aspectos importantes del núcleo esencial, siendo, asuntos importantes del núcleo esencial propios de leyes estatutarias: (i) la consagración de límites, restricciones, excepciones y prohibiciones de alcance general; y (ii) los principios básicos que guían su ejercicio. *(Et al.)* Aspectos todos ellos justamente señalados en relación con el tratamiento de los datos personales de las personas naturales (Sentencia C-748 de 2011).

Es por esta razón que la Corte Constitucional en la misma sentencia termina por señalar, a propósito del núcleo esencial del derecho de Hábeas Data que:

> Así, según la sentencia SU-082 de 1995, el núcleo del derecho al Hábeas Data está compuesto por la autodeterminación informática y la libertad –incluida la libertad económica–. Además, este derecho comprende al menos las siguientes prerrogativas: «a) El derecho a conocer las informaciones que a ella se refieren; b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; c) El derecho a rectificar las informaciones que no correspondan a la verdad.», e incluye el derecho a la caducidad del dato negativo (Sentencia C-748 de 2011).

4.4.1.2 Contenido adyacente: aseguramiento informático o protección de datos personales

Esta segunda dimensión corresponde a la posibilidad que tiene el titular de los datos cuyo tratamiento ha autorizado a un tercero, para exigir que este lo realice tomando todas las medidas necesarias y efectivas para asegurar su confidencialidad, integralidad y disponibilidad, de forma que se evite, por una indebida administración de los mismos, que se le llegue a causar daño. Significa ello gestionar los datos a través de sistemas seguros, acorde a la complejidad o no de la operación en que se involucren. Esta dimensión del Hábeas Data corresponde a aquello que la jurisprudencia refiere como «(...) contenido adyacente objeto de regulación» (Sentencia C-748 de 2011).

4.4.2 EL DATO COMO OBJETO DE PROTECCIÓN DEL DERECHO FUNDAMENTAL AL HÁBEAS DATA

4.4.2.1 Definición del dato

Un segundo elemento del Hábeas Data es su objeto. Pero, si bien el fin último del reconocimiento del Derecho de Hábeas Data lo constituye la protección de la Dignidad Humana, el objeto material de protección propiamente dicho por parte de la normativa que lo regula lo constituyen los datos de las personas naturales, «registrados en bases de datos» (artículo 2.º de la LEPD) cuando de la Ley 1581 de 2012 se refiere, siendo esta última, como se ha advertido en reiteradas ocasiones, el objeto del presente trabajo.

Por tal razón, siendo el dato el objeto de la norma en estudio, cabría precisar previamente el alcance conceptual del mismo, diferenciándolo del concepto de «información». En este propósito, sirve el aporte de la Real Academia de la Lengua Española, quien define dato, en su primera acepción, como: «Antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho» (Real Academia Española, Diccionario de la Lengua Española *(DRAE),* 2012). En tanto que información, en su quinta acepción, se define como «Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada». Es decir que la relación entre dato e

información es de causa a efecto. Por ello podemos decir que con base en los datos (numéricos, alfabéticos, icónicos, etc.) se puede llegar a generar una información (conocimiento) a partir del ejercicio analítico que un sujeto o un sistema ejecuta de aquellos.

En Sentencia T-414 de 1992 la Corte Constitucional se aproximó por primera vez a construir una definición de dato personal, y, apoyada en el concepto rendido a solicitud suya por el profesor Ernesto Lleras, afirmó en ese entonces:

> El dato es un elemento material susceptible de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que el dicho dato adquiera sentido (Lleras *et al.)*. En forma muy somera, se puede decir que el sentido en última instancia, lo producen una o varias mentes humanas y este sentido es un determinante de la acción social. Los modelos se plasman en forma de textos y mensajes que consisten en una serie de signos algunos de los cuales les llamaremos datos, organizados de acuerdo a sistemas de reglas o gramática.
>
> A través de los signos y mensajes los eventos adquieren realidad social. La realidad expresada a través de mensajes… es la determinante de la acción social» (Lleras *et al.,* p. 6).
>
> El dato se constituye entonces en el elemento básico de información sobre eventos o cosas (Fl. 45). (Sentencia T-414 de 1992).

Y agregó la Corte, con citación del profesor Lleras, que:

> El dato que constituye un elemento de la **identidad** de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso. Datos de este tipo serían sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad, y señales de identidad de diversa índole que van emergiendo en las actividades de la vida. Todos estos datos combinados en un modelo, son equivalentes a una «huella digital» porque el individuo es identificable a través de ellos.
>
> Por las **características propias** de los datos, una vez producidos (codificado un evento u objeto por alguien o eventualmente una máquina) pueden diseminarse con relativa facilidad. Esto hace que puedan ser usados, en combinación con otros de procedencias distintas pero adscribibles a la misma persona. Así se va configurando lo que ha dado en llamar un «perfil de datos de una persona» (Lleras *et al.)*. Estos perfiles pueden construirlos quienes tengan bancos de datos bien sea manuales o sistematizados, y el poder de información y control social que estos tengan depende del uso de la tecnología disponible.

> (...) El «perfil de datos» de la persona se constituye entonces en una especie de «persona virtual» sobre la cual pueden ejercerse muchas acciones que tendrán repercusión sobre la persona real. Desde el envío de propaganda no solicitada, hasta coerción u «ostracismo social como en el caso que se presenta. Un «buen» manejo de Bancos de Datos permitiría identificar hasta perfiles poblacionales desde distintos puntos de vista, lo cual constituye un evidente peligro de control social de aquellos que ostentan «poder informático», no solamente contra la libertad de las personas individuales sino contra la de sectores sociales más amplios. (Fl. 46).» (Subrayado de origen) (Lleras *et al.)*.

Por tanto la razón para proteger los datos es justamente porque del proceso asociativo-analítico que de ellos se realiza se puede llegar a obtener, en tratándose de datos personales, información sobre la persona natural a partir de la cual, por un uso inadecuado, pudiera causarse afectación de sus derechos, por sobre todo a los fundamentales.

Cabe decir entonces que, cuando la Ley 1581 de 2012 define el dato personal como «Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables», en realidad está haciendo referencia no a «información» en su sentido semántico, sino más bien referido a los datos (causa de la información) asociados a un Titular. Por ello, se propone definir los datos personales, a fin de evitar confusiones, como el conjunto de las singularidades asociadas a una persona natural que, sometidas a un proceso asociativo-analítico, permiten su individualización frente al resto de la comunidad.

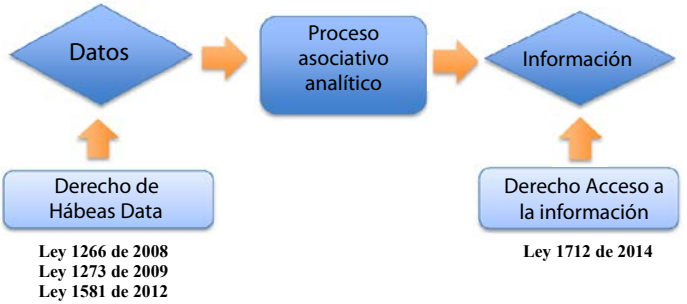


Figura 11. *Relacionamiento dato-información*

«El dato personal debidamente analizado genera información. Sin embargo la ley de Hábeas Data impone obligaciones aún antes de generada esta. Por esta razón el régimen de protección de datos personales en Colombia es uno y el de la información pública otro, aún cuando correlacionados.»

En ese orden de ideas, la información puede ser objeto de clasificación atendiendo, entre otros criterios, a la naturaleza jurídica del sujeto que la posee. Así por ejemplo, se dirá que existe información pública si la misma está en posesión de una entidad pública o de un particular en ejercicio de funciones públicas o surgidas de ejecución de presupuesto público por particulares, en tanto que existirá información privada, si el que la posee es un particular. En tratándose de la información pública hay que señalar que en el caso colombiano, recientemente se han expedido dos normas que regulan su manejo, esto es la Ley 1712 de 2014 denominada Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, cuyo objeto justamente es el de

> regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información» (artículo 1.º Ley 1712 de 2014) y la Ley 1755 de 2015 denominada Ley de Derecho de Petición, «por medio de la cual se regula el derecho fundamental de petición y se sustituye un título del código de procedimiento administrativo y de lo contencioso administrativo.

Adicionalmente, hay que advertir que, tanto la información pública como la privada pueden contener datos de diversa naturaleza. Por ejemplo, la información que un Hospital del Estado (Empresa Social del Estado –ESE–) posee sobre pacientes de VIH, siendo información pública, puede contener datos privados, en este caso incluso de categoría sensibles como lo es el estado de salud del paciente. En tanto que, si se tratara de una clínica particular, la historia clínica del paciente constituirá información privada, aun cuando de seguro pudiera contener datos públicos como lo son por ejemplo el nombre y la cédula del paciente a quien corresponda.

De esta manera, planteada la diferenciación entre los conceptos de información y de datos, habrá de agregarse que la mayor diferenciación entre unos y otros se da en función de la regla general de caracterización de la información pública reservada y no reservada, y caracterización de dato público y no público (semiprivado, privado o sensible).

Obsérvese, para el efecto, que en tratándose de las primeras categorías (información), según la Ley 1755 del 30 de junio de 2015 (artículo 24), «Solo tendrán carácter reservado las informaciones y documentos expresamente sometidos a reserva por la Constitución Política o la ley», *contrario sensu,* la regla general será que si la ley no define su carácter de reservado, se considerará como de acceso públi-

co. Tal presupuesto resulta obvio si se tiene en cuenta que esta regla general busca garantizar el principio de transparencia y el derecho de acceso a la información que maneja el Estado. En cambio, cuando de las segundas categorías (datos) se trata, tal como lo ha señalado en reiterada jurisprudencia la Corte Constitucional, por ejemplo en la Sentencia T-729 de 2002, manteniendo la línea legislativa posteriormente consagrada en la Ley 1266 de 2008 (artículo 3, literal f), la regla general es inversa, pues el dato público «Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política», de donde se deriva entonces que, *contrario sensu,* la regla general será que todo dato es no público, salvo la ley o la Constitución lo califiquen como público. En este caso, se entiende la regla general pues se basa en la obligación constitucional que le asiste al Estado de garantizar el principio de dignidad a partir de la protección de los datos personales de las personas naturales.

TABLA 1. REGLAS DE CARACTERIZACIÓN DE LA INFORMACIÓN Y DE LOS DATOS

Información pública no reservada (Regla General)	**Información pública reservada o clasificada (Excepción)**	**Dato público (Excepción)**	**Dato no público (Regla General)**
Toda la información de la administración pública o de particulares en ejercicio de funciones públicas, que la ley o la Constitución no considere expresamente como reservada.	Sólo aquella información de la administración pública o de particulares en ejercicio de funciones públicas, expresamente señalada por la Constitución o la ley como reservada.	Sólo los datos personales de persona natural, expresamente señalados como tal por la Constitución o la Ley.	Todo dato personal de persona natural que no se considere expresamente por la Ley o la Constitución, como público.

4.4.2.2 Clasificación de los datos personales

Pero efectuadas las anteriores distinciones conceptuales entre dato e información y teniendo clara la dimensión conceptual de la clasifi-

cación entre información pública y privada, la pregunta que cabe ahora formular es: ¿cómo se clasifican los datos personales o con qué criterios lo hace la ley y la jurisprudencia en el caso colombiano? Para dar respuesta al interrogante hay que partir de considerar que clasificar los datos personales es un ejercicio que depende del propósito que se busque con dicha clasificación y por su puesto de los criterios que se adopten para el efecto. Diversos han sido los adoptados para tal finalidad, por ejemplo la naturaleza jurídica de quien trata el dato, el interés del Titular en la divulgación del mismo, el riesgo creado para el titular, la voluntad del constituyente o del legislador, entre otros.

La importancia de la clasificación que se adopte, se traduce en las consecuencias que de ello se derivan, valga decir: si se requiere autorización o no para su tratamiento, los sistemas de aseguramiento físico o virtual de los mismos, la competencia o no de las autoridades administrativas o judiciales para acceder a ellos, entre otras.

Para iniciar se puede afirmar que, una primera categorización de los datos correspondiente al rango más amplio de diferenciación, los clasifica entre datos impersonales y datos personales. Los datos impersonales, son aquellos que no se refieren a una persona (jurídica o natural) en particular. Son ejemplo de ellos el diseño y potencia de una turbina, la composición química de un producto, los códigos fuentes de un sistema informático, entre otros. Este tipo de datos son ajenos al universo de la protección de datos personales (artículo 3, literal e, Ley 1266 de 2008), no obstante ser objeto de protección por otro tipo de normativas, *v. gr.* la Decisión Andina 351 de 1993 que regulan los derechos de autor. Los segundos, o sea los datos personales, son, conforme al literal d del artículo 3 de la Ley 1581 de 2012, «Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables». Estos últimos corresponden al objeto específico de la reglamentación en estudio y sobre los cuales se estará siempre haciendo referencia cuando de dato se hable, salvo expresa advertencia en contrario.

Ahora bien, la clasificación de los datos personales, aun cuando parece un tema sencillo, al realizarse una aproximación a la temática se evidencia su complejidad y la muy poca claridad que al respecto se tiene. Ello se desprende al realizar un cotejo de diferentes hitos clasificatorios que se hubieren presentado. Para poner en evidencia lo afir-

mado, se presenta el siguiente cuadro resumen de los siguientes hitos clasificatorios en el caso colombiano, esto es:

- Sentencia T-729 de 2002.
- Ley 1266 de 2008.
- Sentencia C-1011 de 2008.
- Ley 1581 de 2012.
- Sentencia C-748 de 2011.
- Decreto 1074 de 2015.
- Página web de la Superintendencia de Industria y Comercio.

Primera clasificación, sentencia T-729 de 2002.

Es desarrollada por la Corte Constitucional en la sentencia T-729 de 2002 (refiriéndose a la información y no a los datos quepa advertirlo), donde planteó «(…) cuatro grandes tipos: la información pública o de dominio público, la información semiprivada, la información privada y la información reservada o secreta» y las describió tal cual se aprecia en la figura 11 antes presentada. Este primer intento de clasificación que aborda la jurisprudencia nacional, rescatable en su propósito, por sobre todo en consideración al nivel de desarrollo del instituto jurídico en ese momento, no obstante admite realizarse algunos comentarios sobre la misma:

— En primer lugar, hace sinónimos el término dato e información. De ello se generan confusiones como la que se advierte cuando se lee que la información pública: «puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal», es decir que la información pública puede a su vez ser información privada o personal, lo que constituye un contrasentido jurídico.

— Establece la regla general según la cual si la Ley o la Constitución no definen un dato o información personal como pública, se entenderá que corresponde a cualquier otra tipología pero no a esta.

— Incorpora la definición de «información semiprivada» la información «impersonal» refleja una falta de técnica de redacción toda vez que ésta no forma parte del universo de la protección

de datos, tema abordado en la referida jurisprudencia. Se rescata sí de esta definición, la diferencia práctica entre información semiprivada y privada, al señalar que la primera «solo puede ser obtenida y ofrecida por orden de autoridad administrativa», en tanto que la segunda «solo puede ser obtenida y ofrecida por orden de autoridad judicial». Establece con ello una limitación a la autoridad administrativa en tratándose de información privada y reservada.

— A efectos de definir la categoría del dato semiprivado, incorpora el criterio de «grado mínimo de limitación» para su acceso, constituyendo este un elemento eminentemente subjetivo y de difícil identificación en la práctica.

— En el caso de la información privada, que erróneamente califica como «personal o **no**», nuevamente se identifica confusión de términos entre información y dato, al considerar como ejemplo de ella la historia clínica. La historia clínica efectivamente puede ser información pública o privada (si se atiende a la naturaleza jurídica del Responsable o Encargado) y contener, como en efecto ocurre, datos públicos (nombre, cédula, fecha y lugar de expedición de esta) y datos privados e incluso sensibles como lo sería el estado de salud de quien padece enfermedades, por ejemplo.

— El criterio de identificación de información privada es «el ámbito privado» donde se encuentran la información, criterio que no obstante objetivo no encuentra coherencia con el resto de las categorías. Obsérvese, para sustentar lo dicho que, si entonces una información de «grado mínimo de limitación» para su acceso, pero ubicada en «ámbito privado», sería privado y no semiprivado, lo que resulta poco práctico y generador de confusiones adicionales.

— En tratándose de «información reservada», de la cual considera forman parte los «datos sensibles», afirma que «no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones», mencionando por vía de ejemplo la inclinación sexual o los hábitos. Ante tal afirmación simplemente cabría preguntar si un juez penal, por esta dimensión conceptual que esgrime la Corte Constitucional, no puede realizar pesquisas sobre los hábitos o inclinaciones sexuales del

sindicado de abuso sexual, por ejemplo, lo que resulta inconcebible.

— El criterio de clasificación de la información reservada es el de «estrecha relación con los derechos fundamentales del titular», criterio del cual participan también la información privada como lo es la historia clínica, según el dicho de la misma Corte.

— En conclusión, esta clasificación instrumenta varios criterios de clasificación desarmonizadamente que se traducen en claras incoherencias que impiden su adopción como criterio de actuación de los operadores legales al momento de aplicar de ley.

Segunda clasificación, Ley 1266 de 2008.

Con posterioridad a las precisiones de la jurisprudencia acerca de cómo clasificar los datos, la Ley 1266 de 2008 (artículo 3, literales f, g y h) aportó una **segunda clasificación** con tres y ya no cuatro tipologías de datos, de menor a mayor riesgo en cuanto a su tratamiento, su forma de definición está igualmente en la figura 11. Respecto de este segundo intento de clasificación abordado ahora por la ley, igualmente rescatable, pueden hacerse las siguientes apreciaciones:

— En la ley se avanza en el sentido de precisar ahora ya la referencia al dato y no a la información en general, lo cual abre un camino que se mantendrá con posterioridad, disminuyendo las dificultades advertidas atrás.

— Se mantiene, para el dato público el criterio de identificación de la voluntad constituyente o legislativa, donde por tanto será público aquello que expresamente la ley o la Constitución señale y suma aquellos que por razón de la definición de semiprivados y privados no quepan en dichas categorías.

— Para el dato «semiprivado» se abandona el criterio «grado mínimo de limitación» para su acceso y se sustituye por el de «interés de divulgación» (personal, de grupo o de la sociedad), criterio que refleja tanta dificultad de precisión y por tanto de aplicación como el anterior.

— En relación con el dato «privado» se sustituye el criterio de «estrecha relación con los derechos fundamentales del titular»

por el de «relevancia para el Titular» manteniendo un criterio subjetivo tan ambiguo como el anterior.

— No refiere a datos reservados o sensibles, cuarta categoría advertida por la jurisprudencia del 2002.

— Esta nueva categorización tampoco mantiene claros criterios de clasificación que permitan su adopción como guía de aplicación normativa.

Tercera clasificación, Sentencia C-1011 de 2008.

Surge en la Sentencia C-1011 de 2008, correspondiente al control de constitucionalidad que la Corte Constitucional le hiciera al texto de la Ley 1266 de 2008. Sobre esta clasificación que se puede apreciar también en la figura 11, es preciso realizar las siguientes anotaciones:

— Define como criterio de diferenciación entre dato público y datos semiprivados y privados el «mayor o menor nivel de interés para el titular que tenga la información en ellos contenida», circunstancia que por su profunda subjetividad no permite una real aplicación del criterio.

— Al declarar exequible el artículo 3 literal g) de la Ley 1266 de 2008 correspondiente a la definición de dato semiprivado, determina, en hora buena, que el interés a que hace referencia la norma no es un interés privado, ni cualquier interés público, se trata de «un interés público y objetivo, esto es, relacionado con las actividades sociales que buscan satisfacer finalidades constitucionalmente reconocidas» como lo es por ejemplo la actividad financiera regulada en el artículo 333 de la C. P. de C.

— Señala que el acceso a los datos privados solo es posible por orden judicial, de donde se deriva, *contrario sensu*, que por orden de autoridad administrativa no es posible acceder a ellos, pues por este camino solo se puede acceder a datos públicos y semiprivados, manteniendo la línea de la sentencia T-729 de 2002 manteniendo una línea jurisprudencial en esa dirección.

— Reconoce la existencia de una categoría especial de los datos privados que para el efecto se denominan reservados o sensibles, los cuales, por estar relacionados con el derecho funda-

mental de la dignidad, a la intimidad y a la libertad, su divulgación está proscrita, salvo en materia penal.

— Una vez más se acude a diversos criterios de clasificación combinados, que no dan mucha claridad conceptual, aun cuando aborda con mayor detenimiento el tema que como lo haría años más tarde en la sentencia de control constitucional de la Ley 1581 de 2012 como se pasa a advertir.

Cuarta clasificación, Sentencia C-748 de 2011.

Una cuarta clasificación aparece en la sentencia C-748 de 2011, al momento de resolver la Corte Constitucional la constitucionalidad de la ahora Ley 1581 de 2012. Sobre este pronunciamiento jurisprudencial puede decirse que:

— Con un desarrollo lacónico sobre la clasificación de los datos, incluso restando necesidad a tal ejercicio en el cuerpo de la ley en estudio, y delegándolo más a la jurisprudencia o a la aplicación sistémica del derecho, mantiene la línea de la sentencia C-1011 de 2008 que reconoce tres tipos de datos, acogiendo el criterio de clasificación allí planteado, esto es el de la «aceptabilidad de la divulgación de los datos».

— Afirma que «Los datos personales, a su vez, suelen ser clasificados en los siguientes grupos dependiendo de su mayor o menor grado de aceptabilidad de divulgación: datos públicos, semiprivados y privados o sensibles».

— La falencia del criterio de «aceptabilidad de divulgación» radica en que la subjetividad del mismo no solo está dada por el Titular, sino que también por elementos culturales que pueden variar drásticamente de un lugar a otro de la misma geografía nacional. Sirva de ejemplo el caso de los datos referidos a la condición de hijo extramatrimonial que en comunidades conservadoras como las del altiplano cundiboyacence, es una información muchas veces celosamente guardada, en tanto que en zonas cálidas cercanas a las costas ya no lo es tanto. Igual suele ocurrir con los datos referidos a la condición de unión extramatrimonial, la de hijo extramatrimonial, etc. Todo ello pone en evidencia la fragilidad del criterio adoptado.

Quinta clasificación, Ley 1581 de 2012.

Una quinta, más que clasificación, referencia, la aporta la misma Ley 1581 de 2012 que, como se aprecia en la figura 11, no define sino los datos sensibles manteniendo el sentido de lo expresado en las sentencias T-729 de 2002 y C-1011 de 2008. Por su languidez referencial basta solo señalar que considera a los datos sensibles como datos de categoría especial al igual que los datos de los menores y de los incapaces.

Sexta clasificación, Decreto 1377 de 2013.

El Decreto 1377 de 2013, yendo más allá que la ley reglamentada, esto es la Ley 1581 de 2012, como una sexta clasificación, define el dato público y el dato sensible, omitiendo la definición de los datos privado y del semiprivado, no obstante que los refiere. Esta condición de la ley genera las anotaciones siguientes:

— Aun cuando no define que es un dato semiprivado y un dato privado, si los usa junto con la definición de datos sensibles, como criterio de exclusión de lo que es un dato público, circunstancia que dificulta su comprensión máxime cuando la Ley 1581 de 2012, como se dijo, tampoco hace referencia a estos dos tipos de datos.

— Recoge por vía de reglamentación la definición que la jurisprudencia en las sentencias T-729, C-1011 de 2008 y C-748 de 2008 habían desarrollado sobre dato reservado o sensible en concordancia con la Ley 1581 de 2012.

— De lo advertido se puede afirmar que no presenta una clara definición de criterios clasificatorios de los datos personales.

— (Véase artículo 2.2.2.25.1.3 numeral 2 Decreto 1074 de 2015.)

Séptima clasificación, Superintendencia de Industria y Comercio.

Finalmente, como séptima clasificación de datos se tiene la que presenta en su página web la Superintendencia de Industria y Comercio, máxima autoridad administrativa nacional de control en materia de protección de datos personales en Colombia, refiriendo cuatro ca-

tegorías, esto es dato público, semiprivado, privado y sensible. Al respecto vale decir:

— El criterio que enuncia como determinante de la clasificación es el de «aceptabilidad de la divulgación», al señalar: «Las disposiciones sobre protección de datos, establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación», no obstante tal enunciado no se ve reflejado en las definiciones que aborda posteriormente.

— Se aprecia claramente decantada la diferenciación conceptual entre dato e información.

— Para la definición de dato público se acude al criterio de voluntad legal o constituyente que incorporó la T-729 de 2002, sumando el criterio de exclusión por vía de las órbitas conceptuales de dato semiprivado y dato privado, tal como lo refirió la Ley 1266 de 2008 y que recogió la Sentencia C-1011 de 2008, siendo esta quizá la línea más aceptada hasta la fecha sobre este aspecto.

— Para el dato semiprivado, retoma el criterio de «interés de divulgación» que trae la Ley 1266 de 2008.

— Para el dato privado establece como criterio de identificación la «relevancia exclusiva para el titular» que contiene la Ley 1266 de 2008.

— Para la nueva categoría denominada «dato sensible», que como se dijo o se considera un género de los datos privados (Sentencia T-729 de 2002) o lo mismo que ellos (C-748 de 2011), la SIC adopta el criterio de «riesgo de afectación» para el titular. Es muy importante resaltar que, el aporte que realiza la SIC con este nuevo criterio, es de especial significancia, pues hasta ese momento, ni la ley, ni la jurisprudencia, habían incorporado el criterio «riesgo de afectación» para clasificar un grupo de datos. Con esta incorporación novedosa, en realidad lo que hace la autoridad ambiental, en relación con esta tipología del dato, es trasladar los criterios clasificatorios del campo subjetivo hacia un escenario objetivo. Ya no será, por lo menos en tratándose de datos sensibles la «relevancia para el titular», ni «aceptabilidad de la divulgación» o el «interés de divulgación», el criterio de identificación de dato, sino justamente un criterio más objetivo como lo es el «riesgo de afectación».

— Finalmente hay que afirmar que esta nueva categorización, no obstante su novedad, adolece de similares falencias a las ya mencionadas en anteriores apartes, dificultando en la práctica a las organizaciones seguir con claridad su conceptualización.

No obstante, hay que señalar que el aporte que realiza la SIC con la incorporación del criterio de «riesgo de afectación» lleva a plantearse si el ejercicio que se ha realizado por el legislador, la jurisprudencia y la misma SIC, pudiera tener mejores resultados al momento de intentar la clasificación de los datos incorporando esta noción.

Octava clasificación, propuesta de clasificación a partir del riesgo.

En el propósito de buscar una solución al tema de la clasificación de los datos, tema de importancia como se dijo a efectos de determinar en cada caso cual es el proceder debido por parte del Responsable y del Encargado para cumplir con las «medidas apropiadas y efectivas» que exige el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015, se propone combinar dos elementos objetivos a saber: voluntad del constituyente y/o del legislador, junto con el criterio de «riesgo de afectación», dejando de un lado los criterios subjetivos como el de «relevancia para el titular», «relevancia exclusiva para el titular», «interés de divulgación» y «aceptabilidad de la divulgación», entre otros.

A partir de este propósito por objetivizar la clasificación de los datos, se propone abordar una clasificación que parta solo de dos grandes grupos: (a) datos públicos y (b) datos privados.

Por *datos públicos,* se entenderían todos aquellos datos incorporados en fuentes de información pública o privada, para los cuales la Constitución o la Ley les ha reconocido la calidad de tal. Esta condición permite inferir el principio según el cual cuando de la Constitución o la Ley no pueda tenerse un dato como público, se entenderá que es privado. De esta forma, si un Responsable o Encargado únicamente tratase datos de este tipo, no tendrían que tener autorización de su titular, mucho menos informarle la razón de su tratamiento, ni se le exigirían medidas de protección a los mismos como la incorporación de Sistemas de Gestión de la Seguridad de Datos Personales. En este evento el Estado suple, por vía normativa, la manifestación de voluntad del titular.

Se considerarán datos que forman parte de esta categoría los datos del Registro Civil de las personas pero solo en cuanto refiere al nombre, número de documento de identificación, lugar y fecha de expedición conforme al artículo 51 de la Ley 96 de 1985, la calidad de comerciante conforme al artículo 13 del Código de Comercio, la calidad de profesional conforme al artículo 26 constitucional, la calidad de servidor público conforme a la Ley 909 de 2004, todo en concordancia con el Decreto 1074 de 2015.

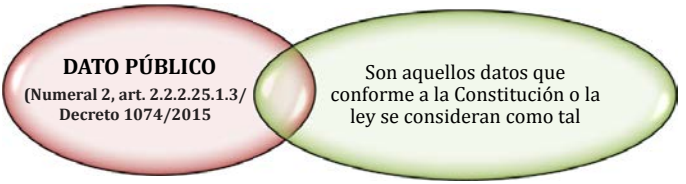


Figura 12. *Datos públicos*

«Los datos públicos no generan para quien los trate ninguna obligación de las surgidas del Hábeas Data.»

Por *datos privados* en tanto, se entenderían todos aquellos datos personales que, como se dijo, no hubieran sido categorizados como públicos por norma alguna. Cuando un Responsable o Encargado trata datos de este tipo, estará obligado necesariamente a adoptar las «medidas apropiadas y efectivas» para proteger a sus titulares. El tratamiento de ellos no podrá darse sin la previa autorización de su titular, salvo eventos excepcionales como: la defensa de intereses superiores del titular o de la sociedad (urgencia médica o sanitaria); la solicitud de información por autoridad administrativa o jurisdiccional en ejercicio de sus funciones legales o en el caso del tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

Ahora bien, en relación con los datos privados se propone subclasificarlos según el nivel de «riesgo de afectación» para el Titular, así: de riesgo alto, de riesgo medio y de riesgo bajo.

Se entenderán como «datos de riesgo alto» todos aquellos datos cuya divulgación, por regla general, pueden constituir causa de discriminación. Para todos los efectos, el concepto de discriminación que aquí se propone corresponde a la definición que el Diccionario de la

Real Academia, en la segunda acepción, ha expresado así: «Dar trato de inferioridad a una persona o colectividad por motivos raciales, religiosos, políticos, etc.». Tal es el caso de los datos ideológicos, de morfología de la persona humana, de salud, etc.

Figura 13. *Datos personales de riesgo alto*

«Los datos privados de riesgo alto se asimilan a los datos sensibles y de personas de especial protección. Constituyen los de mayor riesgo para el titular y por lo tanto mayor exigencia en materia de seguridad para el tratamiento por parte del Responsable o Encargado.»

Por tratarse de datos que exponen en gran riesgo a los titulares, se sugiere que, además de las medidas de seguridad tecnológica que se recomiendan para las otras dos categorías de riesgos (medio y bajo), se sugieren, al menos, las siguientes medidas de seguridad:

— Para el almacenamiento, uso, transmisión o transferencia adecuada y a fin de proteger la integridad de los datos personales de naturaleza sensible, se recomienda la implementación de políticas de controles criptográficos, que establezca los lineamientos para la implementación y gestión de dichos controles.

— Se debe implementar un protocolo de revisión de regularidad de acceso a usuarios, el cual debe contener un registro de control de accesos a los sistemas de información que tratan datos personales, donde se muestre los intentos de acceso, la ID del usuario, fecha y

hora del acceso, sistema de información al que accedió, base de datos, privilegios y la autorización del jefe de proyecto, para efectos de la trazabilidad de las acciones sobre las bases de datos.

— Las copias de seguridad deben estar alojadas en un lugar diferente al Centro de Cómputo principal.

Por otra parte los «datos de riesgo medio» serán aquellos que, de ser divulgados, el riesgo de afectación pueden materializarse en exclusiones (entendida esta en la segunda acepción del Diccionario de la Real Academia de la Lengua Española, que la define como «Descartar, rechazar o negar la posibilidad de algo») que pueden significar para el titular limitaciones al relacionamiento con ciertos actores de la sociedad o afectaciones económicas por impactos en su patrimonio. Por lo general se afectan las posibilidades de los titulares, en términos de la dignidad, para vivir como se debe o como se quiere. Son ejemplo de este tipo de datos los referidos a aspectos económicos o financieros, como el nivel de endeudamiento, historia crediticia, etc. También lo son aquellos datos que refieren procesos en que se hubiera visto involucrado el titular, ya sean de naturaleza penal, administrativa, fiscal o disciplinaria, incluso aún si hubiere sido sancionado. Constituyen parte de esta categoría también las claves de acceso a sistemas informáticos y las direcciones IP, igual que los movimientos transfronterizos del titular, tales como lugares de destino y fechas de salida o reingreso al país, entre otros.

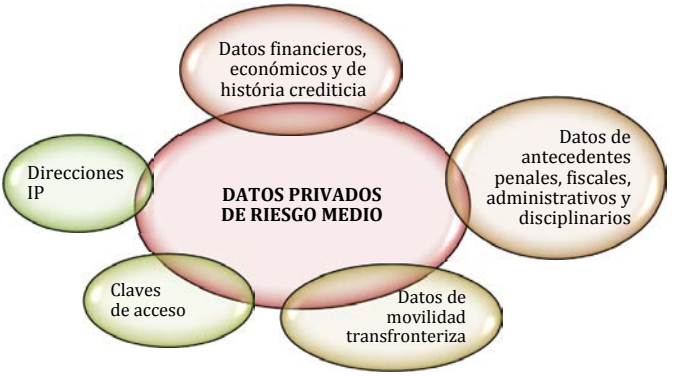


Figura 14. *Datos personales de riesgo medio*

«Los datos privados de riesgo medio, exponen por lo general a su titular a limitaciones de relacionamiento económico.»

Para efectos de la gestión de este tipo de datos, además de las recomendaciones que se advierten para los datos de riesgo bajo, se sugiere implementar, al menos, las medidas siguientes:

a) Los documentos de seguridad deberán contener, además de los dispuesto para el nivel básico, la siguiente información:

— Designación de responsable o responsables de la gestión del documento y de las acciones en él incorporadas.

— Establecimiento de registros de controles para verificar el cumplimiento de lo dispuesto en los documentos de seguridad.

b) El Responsable de los datos personales o el comité de protección de datos personales que se implemente, según la complejidad de la organización, debe designar uno o varios responsables de seguridad y personas encargadas de supervisar la implementación y cumplimiento de las medidas definidas en los documentos de seguridad.

c) Crear procedimientos para la creación y cancelación de usuarios, así como para la gestión de contraseñas de forma personalizada, a los usuarios que intenten acceder a los sistemas de información de la empresa. Adicionalmente, este mecanismo deberá configurarse para limitar los intentos de acceso fallido no autorizado a los sistemas.

d) Crear e implementar políticas de seguridad física y controles de acceso físico a los sitios donde se procesan y almacenan datos personales.

e) Para la gestión de soportes de almacenamiento que requieran ser sacados, se debe establecer un registro de entradas y salidas de los mismos, que permita conocer el tipo de soporte, fecha y hora, datos que contiene, número de soportes, persona a la que se le asigna el soporte y persona que autoriza.

f) Crear protocolos de seguridad para cuando un soporte de almacenamiento requiere ser reutilizado o desechado, debiéndose adoptar medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en el mismo.

g) Implementar el registro de incidentes de seguridad, se deben consignar la fecha en que todos los procedimientos de gestión del incidente son realizados, indicando la persona que ejecutó el proceso y cuál fue la información que se vio comprometida y fue recuperada si ello se ha logrado.

h) Para hacer restauración y/o recuperación de datos desde las copias de seguridad, se debe tener autorización escrita por parte del responsable de los datos personales.

i) Ha de implementarse protocolos para la seguridad de los datos personales cuando son utilizados en pruebas con los sistemas de información. Como regla general no se deben realizar con datos personales reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de datos tratados.

j) Se deben realizar auditorías internas o externas de los sistemas de información y las instalaciones de tratamiento de los datos personales, por medio de registros que verifique el cumplimiento de los lineamientos y procedimientos establecidos en las Políticas y Protocolos de seguridad. Estas auditorías deben hacerse por lo menos cada año y se debe realizar un informe que contenga los hallazgos o no conformidades y proponer las medidas para corregirlas.

Finalmente, se tendrán como «datos de riesgo bajo» todos aquellos que no estando incluidos en las categorías de riesgo alto y medio, no han sido considerados como públicos por la Constitución o la Ley. La divulgación de los datos de riesgo bajo de afectación por lo general generan perturbación a la tranquilidad de los titulares, usualmente con impacto en su intimidad. Es el caso de los datos de identificación contenidos en el Registro Civil referentes a la identidad de las personas, cómo son sus datos biográficos, su filiación y fórmula dactiloscópica; los datos laborales tales como historia de empleo, monto de ingresos, actividades cumplidas; datos de contacto como direcciones físicas o electrónicas, de domicilio comercial o profesional, números telefónicos fijos o móviles, igual que los vinculados con los registros académicos o de calidad profesional.

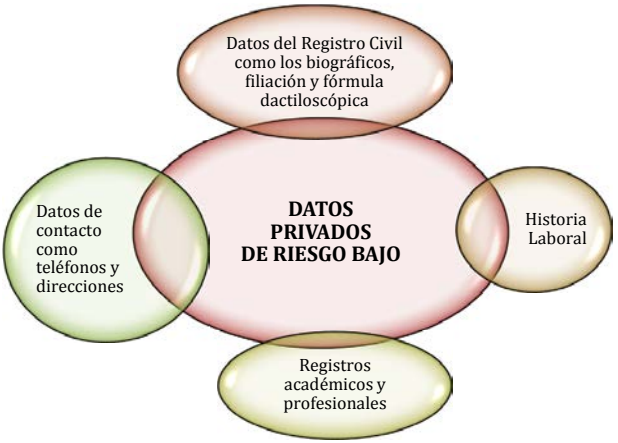


Figura 15. *Datos privados de riesgo bajo*

«Serán, por exclusión, aquellos que no siendo de riesgo alto o medio, no se consideran por la ley o la constitución como públicos.»

Cuando una organización trata datos personales de bajo nivel de riesgo, se sugiere que al menos se adopten las siguientes recomendaciones:

Se debe contar con Políticas y Protocolos de Seguridad de Datos Personales que incluyan, al menos, la siguiente información:

— Ámbito de aplicación de las Políticas y Protocolos especificando detalladamente los recursos protegidos.

— Medidas, normas y procedimientos adoptados para garantizar el nivel de seguridad.

— Roles y responsabilidades del personal para el cumplimiento de las políticas.

— Identificación de las bases de datos que contengan datos personales y descripción de los sistemas de información que los tratan.

— Procedimientos de notificación y gestión de incidentes de seguridad de datos personales.

— Procedimientos para hacer copias de seguridad.

Estos documentos deben mantenerse actualizados y tendrán que ser revisados cada vez que se produzcan cambios significativos en los

sistemas de información o en los elementos que forman parte del sistema interno de datos personales de la organización (titulares, datos, finalidades, procesos, etc.). Así mismo, estos documentos deben ser aprobados por la Alta Dirección, ser implementados y socializarlos con los empleados que tienen acceso a los datos personales dentro de sus funciones.

Se deben definir y documentar claramente las funciones y obligaciones de cada una de las personas que tenga acceso a los datos personales dentro de la Organización, manteniendo en todo momento actualizada la base de datos de los usuarios que tienen acceso a los mismos.

Establecer sistemas de identificación y autenticación de los usuarios con acceso a los datos de carácter personal (Procedimientos de creación de perfiles y gestión de usuarios registrados).

Establecer sistemas de control de acceso a la información que contenga datos personales, con los mecanismos necesarios para impedir que los usuarios tengan acceso a información o recursos a los cuales no están autorizados (Política de Control de Accesos).

Se deben establecer procedimientos para la correcta utilización de soportes de almacenamiento (Protocolo para la gestión de soportes de almacenamiento). Para ello se tendrá en cuenta los dos pasos siguientes:

Se deben tener identificados e inventariados los soportes que alojan datos personales, los cuales deberán almacenarse en un lugar con acceso restringido al personal autorizado.

La salida de soportes que contengan información personal fuera de las instalaciones de la Organización, debe ser autorizada por el Responsable de la base de datos.

Crear e implementar una política de copias de seguridad en la cual se debe garantizar la restauración al estado que estaban en el momento de la ocurrencia de la pérdida o destrucción. Para ello, se deben realizar copias de seguridad una (1) vez a la semana, salvo que en dicho tiempo no se hayan realizado actualizaciones a las bases de datos.

Se deben tener procedimientos de notificación y gestión de incidentes, el cual debe contener un registro en el que se haga constar el tipo de incidencia, el momento en el que ocurrió, la persona que rea-

liza la notificación, a quien se le comunica y los efectos sobre los datos personales que se hubieran derivado de la misma.

Esta clasificación que se plantea y que se advierte posiblemente con menos complejidades que las identificadas en las otras categorizaciones esbozadas, se ha soportado en la línea del pensamiento del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales –INAI–, quien en lugar de categorizar los datos a partir de elementos subjetivos ambiguos y complicados, realiza un planteamiento clasificatorio a partir del mismo criterio esbozado, esto es teniendo en cuenta el riesgo de afectación para el titular. Sirve para ilustrar lo afirmado la *Guía para la Elaboración de un Documento de Seguridad v1.4* de dicha entidad, donde se advierte que:

> Para que el sujeto obligado pueda identificar las medidas de seguridad que resultan aplicables a cada uno de sus sistemas, debe considerar el tipo de datos personales que contiene, lo cual determina el nivel de protección requerido: básico, medio o alto, como a continuación se señala:
>
> 1. *Nivel de protección básico:*
>
> a) Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros.
>
> b) Datos laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
>
> 2. *Nivel de protección medio:*
>
> a) Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.
>
> b) Datos sobre procedimientos administrativos seguidos en forma de juicio y/o jurisdiccionales: Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.
>
> c) Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.
>
> d) Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

3. *Nivel de protección alto:*

a) Datos ideológicos: Creencia religiosa, ideología, afiliación política y sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros.

b) Datos de salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros.

c) Características personales: Tipo de sangre, ADN, huella dactilar u otros análogos.»

d) Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.

e) Vida sexual: Preferencia sexual, hábitos sexuales, entre otros.

f) Origen: Étnico y racial (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales antes IFAI, 2009).

Como puede observarse, el tema del cual ha de ser la más adecuada clasificación de los datos aún está lejos de encontrar terrenos pacíficos, máxime cuando ello estará siempre ligado a los cambios culturales, a los criterios nacionales y a las innovaciones tecnológicas en materia de tratamiento de los datos y de gestión de seguridad de los mismos. Sirve de ejemplo cotejar las notas transcritas de la Guía del IFAI con la propuesta de Metodología de Análisis de Riesgo BAA de la misma institución (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 2014), donde, en esta última se plantea una nueva clasificación, ahora de cuatro categorías, atendiendo a *«la criticidad» de los datos* personales por *«nivel de riesgo inherente»* del mismo. Obsérvese por ejemplo, cómo mientras en la *Guía para la elaboración de un documento de seguridad, vo1.4* se consideran de Nivel de Protección Alto datos como el ADN, la huella dactilar u otros análogos, es decir información física e información biométrica, a la luz de la propuesta de Metodología de Riesgos BAA, serían datos con riesgo inherente medio, circunstancia que pudiera parecer contradictoria.

En conclusión, sobre este aspecto aún falta discusión tanto al interior de las autoridades de protección de datos, como en el campo de la investigación académica y práctica. No obstante, se dejan planteados los criterios de clasificación a partir de combinar el riesgo de afectación y el mandato de la voluntad constitucional o legal, como una al-

ternativa más para aportar a este debate, teniendo siempre presente que, como con acierto comenta el mismo INAI, «ciertos datos personales que en principio no se consideran sensibles, podrían llegar a serlo dependiendo del contexto en que se trata la información» (ibídem).

4.4.2.3 Características del dato personal

Definido como ha quedado el concepto de dato personal y efectuadas las advertencias sobre sus diversas clasificaciones, resulta necesario precisar cuáles son las características propias de estos datos. Para el efecto resulta pertinente acudir a la sentencia T-729 de 2002 que, citada sobre este aspecto en la C-748 de 2011 y apoyándose en las nociones dadas en la sentencia T-414 de 1992, precisó como características de los datos las siguientes:

> 1. «Estar referido a aspectos exclusivos y propios de una persona natural»:
>
> Esta característica no debe entenderse absoluta, pues como la misma Corte Constitucional lo ha manifestado
>
> La definición pareciera reñir, en principio, con algunos pronunciamientos de esta Corporación en los que se ha admitido que las personas jurídicas también pueden ser titulares del derecho al Hábeas Data, como la sentencia T-462 de 1997 y C-1011 de 2008. Sin embargo, en sentir de la Sala, no se trata de una restricción que desconozca la doctrina constitucional sobre la protección del Hábeas Data en cabeza de las personas jurídicas, ni el principio de igualdad. Ciertamente, la garantía del Hábeas Data a las personas jurídicas no es una protección autónoma a dichos entes, sino una protección que surge en virtud de las personas naturales que las conforman. Por tanto, a juicio de la Sala, es legítima la referencia a las personas naturales, lo que no obsta para que, eventualmente, la protección se extienda a las personas jurídicas cuando se afecten los derechos de las personas que la conforman (C-748 de 2011).
>
> 2. (...) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos (C-748 de 2011).

Es decir que en virtud del procesamiento parcial o total de los datos surge la posibilidad de singularizar al sujeto a quien pertenezca la información que de ellos se deriva.

> 3. Su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita» (C-748 de 2011).

Característica que, una vez fue reconocida en el ámbito jurídico, como se ha afirmado en otros apartes iniciales, cambió la concepción histórica según la cual los datos recolectados eran propiedad de quien compraba la base de datos o financiaba su construcción. Hoy quien en calidad de Responsable o Encargado ejerce acciones de tratamiento de datos personales, debe considerarse como un albacea de los datos personales y ya no como propietario de un activo más de su organización.

> 4. Su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación (C-748 de 2011).

Esas reglas y principios que, como se advirtió en el acápite correspondiente, pueden ser: constitucionales, legales o jurisprudenciales, según el marco en que se soporte su existencia o reconocimiento.

4.4.3 EL TITULAR DEL DERECHO DE HÁBEAS DATA Y SUS FACULTADES

El más importante elemento del Hábeas Data, sin lugar a discusión, lo constituye justamente el Titular de los datos personales. Su reconocimiento es de rango constitucional. El artículo 15 superior reconoce tal derecho a *«todas las personas»*, de donde se infiere que, aplicando el principio general de interpretación jurídica según el cual no habiendo distinguido el legislador no le es dado al intérprete distinguir *(Sentencia C-317 de 2012)*, se pregona tanto de la persona natural, como de la jurídica (civiles, comerciales, fundaciones, corporaciones, etc.). En este sentido lo advierte la Ley 1266 de 2008 cuando en su artículo 3.°, de las definiciones, señala que:

> Para los efectos de la presente ley, se entiende por: (a) Titular de la información. Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

Sin embargo, la Ley 1581 de 2012 (LEPD) que como se dijo corresponde a la norma general de protección de datos personales, restringió su ámbito de aplicación solo a los datos de las personas naturales al referir el Titular como la «persona natural cuyos datos personales sean objeto de tratamiento». Esta última circunstancia es la que lleva a advertir que para los propósitos de este trabajo, cada vez que se refiera al Hábeas Data, se estará haciendo referencia al

derecho de las personas naturales, salvo que se efectúe manifestación expresa a las personas jurídicas en cuyo caso habrá de entenderse en los términos de la sentencia C-748 de 2011 antes citada, es decir en la medida en que se vean involucrados derechos fundamentales de las personas naturales que integran las personas jurídicas.

Esta condición de Titular de datos personales que la Constitución Política confiere, otorga un conjunto de atributos que le permite «… conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas», tal como lo preceptúa el artículo 15 constitucional y lo reafirma el artículo 8, literal a, de la LEPD. Pero estas facultades desbordan el contenido gramatical de las manifestaciones normativas, resultando necesario describirlas como a continuación se efectúa:

4.4.3.1 **Facultad de disponer**

Si bien es cierto el artículo 15 superior no refiere expresamente a este atributo del Hábeas Data, es obvio inferir que subyace a la norma misma y que profundiza sus raíces de soporte normativo en los fines perseguidos por el Pueblo de Colombia, manifestado en el Preámbulo, al señalar la expedición de la Constitución de Colombia «con el fin de… asegurar a sus integrantes la vida…, la convivencia…, la igualdad…, la libertad», pues, como ha quedado dicho, la vida, la convivencia, la igualdad y la libertad de las personas quedarían expuestas si no pudiera cada uno definir, por regla general, a quien se le permite acceder a sus propias singularidades, es decir a sus datos personales.

Esto se ve refrendado en los fines del Estado consagrados en el artículo 2.º superior que le señala como deber de las Autoridades, «… proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares», obligación que se ve justamente cumplida entre otras con la expedición de las leyes 1266 de 2008 y 1581 de 2012, junto con sus correspondientes decretos reglamentarios, complementados con la creación de la Autoridad de Control y Vigilancia como lo es la Super-

intendencia Delegada para la Protección de Datos Personales (artículo 19 de la Ley 1581 de 2012).

En virtud de este atributo corresponde al Titular o su representante definir si autoriza o no a un tercero para que realice el tratamiento de sus datos, esto es recolectarlo, almacenarlo, usarlo, circularlo o suprimirlo, esto es lo que se denomina ciclo RAUCS del dato, por las iniciales de cada uno de los verbos descriptores de la actividad correspondiente. Esta facultad de autodeterminación informática propiamente dicha, constituye el *núcleo del derecho del Hábeas Data*. Sin embargo, puede ser objeto de limitaciones o injerencias pero únicamente por mandato legal o por orden judicial (que en últimas le subyace un mandato legal también), en cuyos casos se debe siempre tener en cuenta la armonización con los demás principios superiores constitucionales.

El ejercicio del atributo de disposición del Hábeas Data se materializa y concreta en la autorización que el Titular otorga para que sus datos sean tratados. De igual manera se delimita en razón de la finalidad que Responsable o Encargado, según el caso, advierta como propósito de su recolección. Esta relación *autorización-finalidad* es inescindible, como quiera que la primera siempre lleva ínsita la segunda, debiendo siempre la finalidad ser advertida clara y previamente al Titular (o al menos concomitantemente con la recolección), constituyendo para Responsable y Encargado el rango de acción en el que podrán utilizar legalmente los datos que le han sido confiados, sin que violen los derechos de aquel.

4.4.3.2 Facultad de conocer, también denominado derecho de acceso

En virtud del *principio de transparencia (artículo 4 literal e de la LEPD)*, una vez que el Titular ha ejercido su facultad de autorización e incluso en los eventos en que la manifestación de su voluntad ha sido sustituida por el mandato legal, a él le asiste la facultad de «conocer las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas» (artículo 15 de la C. P. de C. en concordancia con el artículo 14 de la LEPD y los artículos 2.2.2.25.3.7 y 2.2.2.25.4.2 del Decreto 1074 de 2015). No obstante, la facultad que se deriva del Hábeas Data no puede entenderse única y exclusivamente en la dimensión gramatical de la

norma superior. Por tratarse la protección de datos, justamente, de un tema de seguridad, es al Titular, incluso antes que al Estado mismo, a quien corresponde actuar de manera prudente (determinando a quien y en qué circunstancias autoriza o comparte sus singularidades) y vigilante (verificando que se cumpla la ley) respecto de las operaciones que desarrolla el Responsable o el Encargado, para lo cual debe entenderse facultado, como al efecto está, para verificar si sus datos están siendo tratados en debida forma. Es por esta razón que la facultad de conocer debe entenderse extendida a otros asuntos más allá que saber qué datos del Titular han sido recolectados. La Agencia Española de Protección de Datos por ejemplo define el derecho de acceso en los siguientes términos:

> Es uno de los derechos que la Ley Orgánica de Protección de Datos de carácter personal (LOPD) reconoce a los ciudadanos para que el ciudadano pueda controlar por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a obtener información sobre si éstos están siendo objeto de tratamiento y, en su caso, la finalidad del mismo, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos (http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/acceso-ides-idphp.php).

Por lo antes expuesto, dentro de los varios asuntos que la facultad de conocer le permite al Titular indagar a quien trata sus datos personales, ya sea a través de consulta ejercida por vía de derecho de petición (artículo 23 de la C. P. C.) si fuere necesario o incluso por vía de Tutela (artículo 86 de la C. P. C.) si aquel no fuere atendido no obstante su obligatoriedad (artículo 11 de la LEPD en concordancia con los artículos 2.2.2.25.4.1 al 2.2.2.25.4.4 del Decreto 1074 de 2015), se pueden mencionar:

- *La autorización.*

No obstante parecer obvio que si se requiere de la autorización para tratar los datos personales del Titular, este la conoce, pueden ocurrir circunstancias en que los datos sean tratados por quien directamente no resultó autorizado y por lo tanto, ante una interacción entre este y el Titular, podría solicitar incluso la copia de la misma para efectos de determinar con que autorización los está tratando. Es el caso común de interacción de Titulares con Encargados o el de terceros que tratan datos no autorizados por el Titular, ante quienes, en virtud de la facultad de conocer, podría solicitar copia de la autoriza-

ción ya sea para constatarla o, ya para poner en evidencia la ilicitud del tratamiento (artículo 8 literal b de la LEPD en concordancia con el artículo 2.2.2.25.2.5 del Decreto 1074 de 2015).

- *La finalidad y tratamiento.*

Al igual que la autorización, la finalidad y el tratamiento se presuponen conocidas por el Titular desde el momento en que se capturan los datos. No obstante, en cualquier momento el Titular se encuentra facultado para solicitar al Responsable o al Encargado se le informe la finalidad para la cual se le autorizó el tratamiento correspondiente y el tratamiento mismo que les da a los datos (art. 12 literal a de la LEPD). No debe confundirse la finalidad con el tratamiento. La finalidad, como se dijo se asimila a la causa del contrato de tratamiento de datos. En el caso del contrato principal de Hábeas Data, la finalidad puede ser la conformación de bases de datos con propósitos definidos como actividades de comercialización, sondeos de opinión, entre otros. En el caso del contrato accesorio de Hábeas Data, puede ser finalidad el facilitar la celebración o ejecución del contrato principal al cual está adherido jurídicamente, por ejemplo, los datos laborales para el contrato de trabajo. El tratamiento, en cambio lo constituye cualquier actividad, organizacionalmente adoptada o legalmente ordenada, susceptible de enmarcarse dentro del ciclo RAUCS, esto es recolección, almacenamiento, uso, circulación o supresión de los datos. Esta posibilidad para el Titular de poder conocer tanto finalidad como tratamiento, se deriva entre otras del mandato normativo contenido en el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, según el cual la Política de Tratamiento de la Información –PTI– debe contener tal información cuando no se hubiera dado a conocer en el Aviso de Privacidad (artículo 2.2.2.25.3.4 y 2.2.2.25.3.5 del Decreto 1074 de 2015), ambos documentos que deben ser publicitados de forma que el Titular los conozca.

Mecanismos de seguridad: Está definido conforme al principio de seguridad, como obligación de Responsables y Encargados, tratar los datos que se le autoriza con «las medidas técnicas, humanas y administrativas que sean necesarias» (artículo 4 literal g de la LEPD), para brindarles la seguridad que permita la confidencialidad, la integralidad y la disponibilidad de los mismos. Frente a esta obligatoriedad, cabría preguntarse si puede el Titular solicitar infor-

mación sobre los aspectos técnicos utilizados por el Responsable o Encargado para cumplir con tal carga obligacional. Al respecto hay que decir que, debiéndose reportar aspectos sobre la seguridad tecnológica ante el Registro Nacional de Bases de Datos que la Superintendencia de Industria y Comercio ha establecido en cumplimiento del Decreto 1074 de 2015 y reglado con la Circular Externa No. 2 del 03 de noviembre de 2015 (Superintendencia de Industria y Comercio, 2015), la que es de suyo un registro público, con mayor razón podría el Titular directamente auscultar sobre estos aspectos. Sin embargo, ha de tenerse siempre presente la ponderación que habrá de hacerse del derecho de acceso del Titular y el derecho a los secretos industriales de los Responsables y Encargados que pudieran verse expuestos ante tales peticiones. En este sentido cabe referir lo expresado por la Directiva 95/46 de CE que al respecto manifiesta: «que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan, al menos en el caso de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; que este derecho no debe menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informático; que no obstante esto no debe suponer que se deniegue cualquier información al interesado» (Unión Europea, 1995).

- *Usuarios autorizados.*

Al interior de las organizaciones, en el desarrollo diario de sus operaciones, no todos los roles desempeñados por los empleados de aquellas, tienen funcionalmente hablando, autorización para acceder a los datos personales que se tratan. Por ello, la definición de roles y competencias en relación con procesos que involucran datos personales al interior de las organizaciones, es esencial para efectos de asegurarse el principio de acceso y circulación restringida según el cual el tratamiento «solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas» (artículo 4.º, literal f de la Ley 1581 de 2012) en la ley. Sin embargo, estima que la posibilidad de inquirir sobre estos aspectos solo le sería posible al Titular en los eventos de discusiones en el campo jurisdiccional o administrativo, caso en el cual en últimas quien termina solicitando la información lo será el juez o funcionario correspondiente.

- *Ubicabilidad.*

Frente a la prohibición de transferencia de datos a países que no brinden similares garantías que las colombianas en materia de protección de datos (art. 26 de la LEPD), el Titular de los datos sin lugar a dudas podrá solicitar información acerca de si sus datos están siendo objeto de dicho tratamiento (transferencia o transmisión nacional o internacional), entre otras por cuanto de ser así, sin que se hubiere dado su autorización, se estarían violando sus derechos y los principios que rigen la materia. Podrá incluso el Titular solicitar que se le informe sobre la existencia o no del contrato de transmisión de datos personales de que trata el artículo 2.2.2.25.5.2 del Decreto 1074 de 2015. De hecho, sobre este último aspecto, en la plataforma tecnológica del RNBD que ha dispuesto la Superintendencia de Industria y Comercio en su página web en el enlace http://www.sic.gov.co/drupal/registro-nacional-de-bases-de-datos, se ha incorporado esta circunstancia dentro de la información que debe darse sobre las bases de datos que se registren.

- *Los datos.*

Aunque resulta obvio, no sobra advertir que será facultad del titular indagar acerca de cuáles son los datos (art. 14 de la LEPD) que un determinado Responsable o Encargado está tratando y cual el uso que le han dado (art. 8, literal c, y art. 17, literal m, de la LEPD), entre otras para efecto de poder verificar si aquello que ha autorizado está en concordancia con aquello que efectivamente se está realizando. Esta posibilidad permite, entre otras, al Titular asegurar para sí el cumplimiento del principio de individualidad que como se dijo busca «mantener separadamente las bases de datos (…) de tal forma que queda prohibida la conducta dirigida a facilitar cruce de datos a partir de la *acumulación* de informaciones provenientes de diferentes bases de datos». (Sentencia T-729 de 2002)

4.4.3.3 **Facultad de actualizar y/o rectificar**

En virtud del *principio de veracidad* y calidad de los datos, los Responsables y Encargados están obligados a asegurarse que la información tratada sea, entre otras, «veraz, completa, exacta, y actualizada» *(artículo 4 literal d de la LEPD),* circunstancia que deviene en el

hecho de poder el Titular exigir o reclamar que la información que sobre él se trata refleje el estado actual de la situación del dato *(art. 15 de la LEPD)*. Es típico caso de esta circunstancia, por ejemplo, lo que ocurre con los operadores de información (centrales de riesgos) ante quienes las fuentes (entidad financiera) reportan la historia crediticia de uno de sus obligados, sin realizar los ajustes que se van dando con ocasión de las acciones de pago de aquel. Otro ejemplo se configura en tratándose de datos asociados a la salud, frente a eventos de diagnósticos iniciales de patologías que, se dejan registrados en la historia clínica de una determinada institución, sin corrección posterior cuando resultan desvirtuados. En uno y otro caso la falta de veracidad de los datos puede generar graves consecuencias al titular (no acceso a crédito por reporte de mora ya superada o declaratorias, sin razón, de preexistencias frente a seguros médicos o de vida). Por tal motivo al Titular le asiste la facultad de reclamar que sus datos estén siempre conforme a la realidad y debidamente actualizados.

4.4.3.4 **Facultad de oposición**

Fundamentado en el principio de libertad consagrado en el literal c del artículo 4 de la ley 1581 de 2012, el Titular del dato, salvo obligación legal o contractual, puede negarse a que sus datos sean tratados, es decir oponerse a que un tercero conserve y utilice sus singularidades. Pero esta facultad implica igualmente que, habiendo autorizado su uso, pueda posteriormente el Titular expresar su deseo por revocar dicha autorización o lo que es lo mismo solicitar la supresión de los datos. La Ley 1581 de 2012 condiciona el ejercicio de la revocatoria y/o supresión al evento en que no se respeten los principios, derechos y garantías constitucionales y legales. En similares términos lo explica la Agencia Española de Protección de Datos cuando define la facultad de oposición como

> el derecho a que no se lleve a cabo el tratamiento de éstos o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario (Agencia Española de Protección de Datos, 2014).

Sin embargo, se considera que tales circunstancias o motivos legítimos no constituyen requisito *sine qua non* para que el Titular solicite la supresión del dato, cuando no exista ley que legitime al Respon-

sable o Encargado para conservarlo. Justamente por razón del principio de autodeterminación informática que inspira el principio de libertad, se deriva que, si no existe obligación legal para que el Responsable conserve los datos o han cesado las razones contractuales que lo motivaban, no será necesario para el Titular esgrimir razón alguna para la oposición o solicitud de supresión, más que su propia voluntad.

La facultad de oposición también se expresa en la posibilidad que le asiste al Titular para condicionar el tratamiento al momento de emitir su autorización. En virtud de ello, por ejemplo, puede el Titular prohibir la transmisión internacional de sus datos, la cesión de los mismos o, lo que se ha vuelto tan usual y profundamente incómodo, casi violatorio de la intimidad, la utilización de datos de contacto en horarios y días no laborales, v. gr. domingos o festivos en horas nocturnas o a primeras de las mañanas.

El responsable o encargado, en muchos casos incluso, no deben esperar la solicitud de supresión del dato, pues debe acatar el fenómeno de la caducidad del dato, esto es la eliminación unilateral de los datos cuando un tiempo legal, contractual o la razonabilidad de su naturaleza y uso lo indican. Constituye ejemplo de lo afirmado lo advertido por la Corte Constitucional en tratándose de datos financieros al afirmar:

> El término para la caducidad del dato lo debe fijar, razonablemente, el legislador. Pero, mientras no lo haya fijado, hay que considerar que es razonable el término que evite el abuso del poder informático y preserve las sanas prácticas crediticias, defendiendo así el interés general. Si el pago se ha producido en un proceso ejecutivo, es razonable que el dato, a pesar de ser público, tenga un término de caducidad, que podría ser el de cinco (5) años. Sin embargo, cuando el pago se ha producido una vez presentada la demanda, con la sola notificación del mandamiento de pago, el término de caducidad será solamente de dos (2) años, es decir, se seguirá la regla general del pago voluntario (SU-082 de 1995 Corte Constitucional).

4.4.4 CONTRATO DE HÁBEAS DATA

Un cuarto elemento del Hábeas Data, lo constituye el contrato mismo de Hábeas Data o negocio jurídico de disposición de datos personales. Por ello se afirma que, en tratándose del Titular persona

natural, hay que tener en cuenta que en virtud del ejercicio de la autonomía de la voluntad, cuando aquel autoriza a otro el tratamiento de sus datos personales, en realidad está realizando un negocio jurídico, el que se propone denominarse *Contrato de Hábeas Data* y que, en concordancia con el artículo 1495 del C. C., una parte se obliga (para el efecto el Responsable o Encargado) para con otra (esto es el titular) a *hacer* el tratamiento de los datos conforme a la finalidad para la cual los captura y con los mecanismos de seguridad apropiados. Adicionalmente también se obligan a *no hacer* divulgación o facilitar el acceso a terceros no autorizados, ni dar uso diferente de aquel para el cual fue recolectado, todo en el marco de las disposiciones constitucionales, legales y reglamentarias que regulan justamente el Derecho de Hábeas Data.

De la anterior afirmación se colige que para que sea válido este negocio jurídico, representado en la autorización y posterior entrega de datos personales a un tercero para su tratamiento, se deben cumplir las exigencias del artículo 1502 del C. C. a saber:

4.4.4.1 Capacidad del titular

Esto significa que quien autoriza el tratamiento de sus datos debe ser una persona mayor de edad (18 años o más) y no estar incurso en ninguna de las causales de incapacidad, como pudiera ocurrir a la persona que se encuentre en condición de discapacidad mental absoluta o en condición de incapacidad fono-auditiva sin que pueda darse a entender, al igual que los disipadores bajo estado de interdicción (artículos 1503 y 1504 del C. C. en concordancia con la Ley 1306 de 2009). En tratándose de incapaces absolutos la disponibilidad del dato estará en cabeza de quien ejerce su representación legal (tutor, curador o titular de la patria potestad).

Si se trata de un titular menor de edad, se deberá tener en cuenta que cuando el artículo 7 de la LEPD hace referencia a niños, niñas y adolescentes lo hace en los términos de la Ley 1098 de 2006 (Código de Infancia y Adolescencia), razón por la cual siempre que se refiera al acto de disposición de los datos personales no se hará distinción alguna entre las mencionadas categorías. Por tal razón, para efectos del Hábeas Data, por menor de edad se entenderán incluidos todas las personas menores de 18 años. Debe resaltarse además que aun

cuando la norma manifiesta que «*queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes*», esta disposición ha de interpretarse como que

> los datos de los niños, las niñas y adolescentes pueden ser objeto de tratamiento siempre y cuando no se ponga en riesgo la prevalencia de sus derechos fundamentales e inequívocamente responda a la realización del principio de su interés superior, cuya aplicación específica devendrá del análisis de cada caso en particular (Sentencia C-748 de 2011).

Esta advertencia de la Corte Constitucional, fundada en el artículo 44 superior, debe entenderse como que, por tratarse de población de protección constitucional reforzada, siempre que se traten datos personales de menores, se deberá tener en cuenta el principio de «interés superior del menor», lo cual significa:

> (i) Garantía del desarrollo integral del niño. Se debe, como regla general, asegurar el desarrollo armónico, integral, normal y sano de los niños, desde los puntos de vista físico, psicológico, afectivo, intelectual y ético, así como la plena evolución de su personalidad (…).
>
> (ii) Garantía de las condiciones para el pleno ejercicio de los derechos fundamentales del niño. Los derechos de los niños deben interpretarse de conformidad con las disposiciones de los tratados e instrumentos de derecho internacional público que vinculan a Colombia (…).
>
> (iii) Protección del niño frente a riesgos prohibidos. Se debe resguardar a los niños de todo tipo de abusos y arbitrariedades, y protegerlos frente a condiciones extremas que amenacen su desarrollo armónico, tales como el alcoholismo, la drogadicción, la prostitución, la violencia física o moral, la explotación económica o laboral, y en general, el irrespeto por la dignidad humana en todas sus formas (…).
>
> (iv) Equilibrio entre los derechos de los niños y los derechos de sus padres, sobre la base de que prevalecen los derechos del niño. Es necesario preservar un equilibrio entre los derechos del niño y los de los padres, pero cuando quiera que dicho equilibrio se altere, y se presente un conflicto que no pueda resolverse mediante la armonización en el caso concreto, la solución deberá ser la que mejor satisfaga el interés superior del niño (…).
>
> (v) Provisión de un ambiente familiar apto para el desarrollo del niño. El desarrollo integral y armónico de los niños (art. 44 CP), exige una familia en la que los padres o acudientes cumplan con los deberes derivados de su posición, y le permitan desenvolverse adecuadamente en un ambiente de cariño, comprensión y protección (…).
>
> (vi) Necesidad de razones poderosas que justifiquen la intervención del Estado en las relaciones paterno/materno-filiales. El solo hecho de que el niño pueda estar en mejores condiciones económicas no justifica de por

> sí una intervención del Estado en la relación con sus padres; deben existir motivos adicionales poderosos, que hagan temer por su bienestar y desarrollo, y justifiquen las medidas de protección que tengan como efecto separarle de su familia biológica *(et al.)* (Sentencia C-748 de 2011).

4.4.4.2 Consentimiento del titular, exento de vicio

El consentimiento, esto es la manifestación de la voluntad de parte del Titular para autorizar que sus datos sean tratados, deberá ser expresada, por regla general, por él o por intermedio de apoderado o representante legal, o, en caso de muerte, por sus causahabientes, tal como se desprende del artículo 5 en concordancia con el artículo 2.2.2.25.4.1 del Decreto 1074 de 2015. Surge en todo caso, de esta última disposición referida, el interrogante de si, ¿una persona que no ostenta ninguna de las condiciones antes mencionadas, puede expresar el consentimiento «a favor de otro o para otro» (artículo 1506 del C. C.), para permitir que un tercero trate los datos personales sin que el Titular hubiere autorizado? Para responder este interrogante se debe partir de la regla general enunciada para la cual se propone, como excepción muy especial la aceptación de esta circunstancia para aquellos eventos en que se encuentre en riesgo inminente de vulneración derechos fundamentales por la omisión en la entrega de datos personales. Este es por ejemplo el caso de intervenciones quirúrgicas de emergencia donde familiares o incluso terceros, conocedores de datos personales de la víctima (enfermedades que padezca el paciente, sus creencias religiosas, tipo de sangre, etc.) los suministren para efecto de su adecuada intervención u, otro caso, en el evento de requerirse asegurar el acceso a la educación de un menor (interés superior de sujeto de especial protección) un tercero provee datos del menor a un establecimiento educativo para asegurar el ingreso al mismo ante el riesgo de vencimientos de plazos de matrícula. En estos casos excepcionales, se requerirá que el titular o su representante legal, con posterioridad, convaliden la autorización dada a efectos de poder continuar con el tratamiento posterior de los datos así recolectados.

La falta de consentimiento solo es reemplazable por la manifestación de voluntad del Estado a través de mandato legal que califique como público un determinado dato, autorice a autoridad administrativa o judicial para acceder a ello o la ley lo considere como excepción (artículo 2.2.2.25.2.1 del Decreto 1074 de 2015 en concordan-

cia con el artículo 10 de la LEPD). Hay que señalar que en los casos en que la voluntad del Estado faculte a las autoridades administrativas o judiciales a tratar datos sin la voluntad del titular, contrario a lo erróneamente considerado por algunos administradores públicos, estos deben cumplir con las demás exigencias que en materia de tratamiento de datos personales se exige en la ley. En otras palabras, aun cuando la ley faculte el acceso a datos personales de un Titular, obviamente distintos a datos públicos, quien desarrolla dicho tratamiento (sea persona pública o privada), en todo caso deberá implementar los mecanismos necesarios y efectivos para garantizar a los titulares el respeto de sus derechos.

Ahora bien, en todo caso, cualquiera sea la circunstancia de la expresión del consentimiento para el tratamiento del dato personal, es decir, bien sea directamente o por interpuesta persona, este deberá ser manifestado de forma libre de error, fuerza y dolo, en los términos del artículo 1508 del C. C., es decir sin vicio que pueda constituir causal de nulidad. Adicionalmente, en tratándose de los casos en que el mandato legal autoriza a la administración, deberá esta poner de presente la competencia legal con base en la cual pretende ejercer de manera coactivamente el tratamiento.

El consentimiento expresado para el caso de los datos personales, conforme al *principio de libertad* consagrado en el artículo 4 literal c de la LEPD, debe ser un *consentimiento calificado,* es decir que para efecto de evitar su invalidez el mismo debe cumplir con las condiciones particulares siguientes:

a) Debe ser expresado, «a más tardar en el momento de la recolección» de los datos (artículo 2.2.2.25.2.2 del Decreto 1074 de 2015), salvo en los eventos excepcionales advertidos de la estipulación a favor de otro o para otro o cuando lo sustituye el Estado por mandato legal o judicial. Son antecedentes de esta línea jurisprudencial que exige consentimiento previo, la Sentencia T-022 de 1993 y T-592 de 2003, entre otras.

b) Ha de hacerse constar por escrito, oral o por conductas inequívocas del Titular, pero siempre teniendo en cuenta que:

> (…) no está permitido el consentimiento tácito del Titular del dato. El consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales (Sentencia C-748 de 2011).

Son antecedentes de esta línea jurisprudencial que demanda consentimiento expreso, las sentencias T-580 de 1995, T-580 de 1995 y T-657 de 2005, entre otras.

c) Y en todo caso, al Titular ha de informársele, como lo ha señalado la Jurisprudencia Constitucional,

> (…) ante quien, desde cuándo y por cuánto tiempo su autorización será utilizada, porque una aquiescencia genérica no subsume el total contenido de la autodeterminación informática, prevista en la Carta Política para que a los asociados les sea respetada su facultad de intervenir activamente y sin restricciones, durante las diversas etapas del proceso informático (Sentencia T-592 de 2003).

Por ello, en el artículo 12 de la LEPD se determinó que el Responsable (y aun cuando no se dice, también el Encargado si es quien recolecta el dato) deberá informar de manera clara y expresa al Titular la siguiente información: *«a.* El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo».

Sobre este apartado debe señalarse que, tal cual lo advierte la norma, ha de informarse, por una parte, el tratamiento que se dará a los datos y, por la otra, la finalidad del para qué se recolectan. Se realiza esta advertencia, que parece superflua, por cuanto se observa en la práctica muchos casos en que la autorización solo informa la finalidad (enviar ofertas comerciales, asociar los resultados académicos a los alumnos, definir el acceso a beneficios de un determinado sistema, etc.) sin que se refiera al tratamiento que se dará a los mismos, tratamiento que está ligado al ciclo del dato, esto es recolección, almacenamiento, uso, circulación o supresión.

> b. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
>
> c. Los derechos que le asisten como Titular;
>
> d. La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

El consentimiento calificado o autorización emitido por el Titular o su representante es de tal importancia que, incluso si el Responsable del Tratamiento o el Encargado realiza actividades por cuenta de aquel, deberá conservar la prueba del mismo para aquellos eventos en que el Titular le solicite copia de esta o para los eventos en que la Superintendencia de Industria y Comercio lo exija como documento

de *accountability* o responsabilidad demostrada. También deberá tenerse presente la autorización al momento de inscribir las bases de datos (obligación surgida del Decreto 1074 de 2015 en concordancia con la Circular Única en su Título V, capítulo 2.º) como quiera que, con el propósito de fiscalizar esta labor, en la plataforma web dispuesta por esta entidad para el Registro Nacional de Bases de Datos –RNBD–, se interroga al respecto los siguientes asuntos: ¿Cuenta con autorización? (¿si, no, en algunos casos?), ¿Cuál es la forma de obtención de los datos? (es gratuita, con contraprestación, por cesión, directamente por del Titular o de fuente pública) y, si aplica, ¿Existe alguna causal de exoneración de autorización? (Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, Datos de naturaleza pública, Casos de urgencia médica o sanitaria, Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos, Datos relacionados con el Registro Civil de las personas).

4.4.4.3 **Objeto del tratamiento del Hábeas Data**

Conforme al artículo 1517 del C. C., el objeto de la declaración de voluntad lo será «una o más cosas, que se trata de dar, hacer o no hacer». De esta forma, en cuanto se refiere a la voluntad manifiesta del Titular del dato en relación con el Contrato de Hábeas Data, el objeto de la misma lo serán los datos personales. Pero entendido como está que estos no son cosa diferente que las singularidades del Titular, como quedó dicho en las primeras páginas de este trabajo, de ellos en sí mismos no se podrá pregonar ilicitud alguna. Recuérdese que los datos personales constituyen una extra corporeidad del ser humano, que son objeto de especial protección, entre otras para efectos de proteger la dignidad de aquél a quienes refiere, es decir evitar su exclusión, asegurar su plan de vida y permitirle vivir como se debe.

Por tal razón, de singularidades como el nombre, la identificación, los datos de contacto, la información financiera, la ideológica, la religión, el ADN, la huella dactilar, el iris, etc., no es posible predicar ilicitud alguna. En consecuencia, respecto de este elemento del negocio jurídico de tratamiento de datos personales hay que advertir que siempre implicará objeto lícito.

4.4.4.4 Causa del tratamiento del Hábeas Data

La causa del tratamiento lo constituye el motivo, conocido por el Titular y por el Responsable o el Encargado, que lleva al primero a confiar al segundo sus singularidades personales. Así por ejemplo el anhelo o la necesidad de acceder al servicio de salud de parte del Titular y el propósito de prestarla por parte del Responsable o Encargado, constituye la causa del negocio jurídico de tratamiento de datos personales del primero. Igual ocurre con el estudiante y la institución educativa en cuanto al servicio de educación, el acreedor y la entidad financiera en cuanto a los servicios bancarios, entre otros.

No obstante, siempre el objeto ser lícito, como se advirtió en acápite anterior, cuando nos detenemos a precisar cuáles pueden ser las causas comúnmente conocidas por el Titular de los datos y el Responsable o Encargado de los mismos, para convenir el tratamiento de aquellos, deben precisarse circunstancias de cada caso, pues de darse alguna constitutiva de ilicitud invalidaría el acuerdo celebrado. Tal sería por ejemplo el caso de autorización del tratamiento de datos personales con el propósito de desarrollar conductas como la *inducción a la prostitución (artículo 213 del C. P.)* o el aberrante caso del representante del menor quien autorizara el tratamiento de datos personales de este para actividades asociadas a la *pornografía con personas menores de 18 años (artículo 218 del C. P.)* O de *utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores (artículo 219.ª del C. P.)*.

Las referencias efectuadas en torno a la causa del negocio jurídico de tratamiento de datos personales ponen de relieve que el negocio mismo puede tener, en los términos del artículo 1499 del C. C. una doble manifestación, es decir, que puede ser o bien un contrato principal o bien un contrato accesorio. El primer evento (contrato principal) se da cuando la razón o causa del contrato lo constituye la construcción misma de la base de datos, caso por ejemplo de aquellas que se elaboran para efectos de mercadeo, donde el titular autoriza ser incluido dentro de ella para efectos de recibir información de productos, ofertas, etc. En este caso la causa suficiente para que el contrato cumpla con este presupuesto de validez lo será el simple anhelo de participar de una relación jurídica de comunicabilidad. El segundo caso (contrato accesorio) será aquel en el cual la

base de datos se construye para efectos de facilitar la ejecución de otro contrato, como por ejemplo cuando se construye la base de datos de los empleados de una empresa, en cuyo evento el contrato principal lo será el correspondiente contrato de trabajo, o en el caso de las bases de datos de los compradores de tiquetes de transporte, en cuyo caso el contrato principal será el de transporte de pasajeros, o cuando se levantan datos de los cuentacorrentistas, donde el contrato principal lo será el bancario de cuenta corriente, siendo por tanto el de tratamiento de datos accesorio a todos ellos. En estos eventos vale recordarse que la suerte de lo principal lo corre lo accesorio, de donde se deriva que todo cuanto afecte la validez del contrato principal, afectará el correspondiente de tratamiento de datos personales.

La causa del contrato, por lo afirmado, está íntimamente ligada con la autorización (cuando esta no está sustituida por el mandato legal o judicial) pues define el marco referencial del tratamiento en virtud del principio de finalidad. Esto explica la prohibición de la recolección de datos sin causa que lo motive, tal cual lo ha señalado la jurisprudencia constitucional al afirmar:

> Según el principio de finalidad, tanto el acopio, el procesamiento y la divulgación de los datos personales, debe obedecer a una finalidad (…) constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista (…) Según el principio de utilidad, tanto el acopio, el procesamiento y la divulgación de los datos personales, debe cumplir una función determinada, como expresión del ejercicio legítimo del derecho a la administración de los mismos; por ello, está prohibida la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara o determinable. (Sentencia T-729 de 2002)

4.4.5 RESPONSABLES, ENCARGADOS Y SUBENCARGADOS

El quinto elemento del Hábeas Data será la contraparte del Titular del dato en el contrato (principal o accesorio) de Hábeas Data que, como ha quedado advertido, lo serán el Responsable, el Encargado y el Subencargado.

Conforme al artículo 3, literal e, de la LEPD, se entiende por Responsable del Tratamiento a toda

> Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos». El elemento determinador de la calidad de Responsable estará dado por «la posibilidad de definir –jurídica y materialmente– los fines y medios del tratamiento (Sentencia C-748 de 2011).

Criterio acogido por la Corte Constitucional, entre otras siguiendo la línea conceptual de la Directiva 95/46/CE y en el Dictamen 1/2010 del Grupo Consultivo sobre Protección de Datos.

Tres son las condiciones en virtud de la cuales se puede considerar que una determinada persona asume el rol de Responsable, es decir la competente para resolver sobre «las cuestiones de fondo que sean esenciales a efectos de la legitimidad del tratamiento» (Directiva 95/46/CE), como lo refiere la Corte Constitucional (Directiva 95/46/CE) siguiendo la Directiva europea:

1. Por competencia legal explícita: Corresponde a los eventos en los cuales la ley impone la función de recolección de datos. Es por ejemplo el caso de las funciones de fiscalización que ejecuta la Dirección de Impuestos y Aduanas Nacionales –DIAN– en Colombia, por virtud de las cuales puede acceder y recolectar datos financieros (datos semiprivados) de los contribuyentes o en el caso de las entidades del sistema de la Seguridad Social en cuanto a las historias laborales (datos semiprivados) para efectos pensionales.

2. Por competencia jurídica implícita: Se presenta en los eventos en que por razón de las acciones propias de una determinada actividad surge el imperativo del tratamiento de datos personales. Es por ejemplo el caso de la información de salud de un paciente y su médico, el Colegio y los datos del estudiante o el empleador con los del trabajador. Esta condición es típica de las relaciones que se han denominado en el presente trabajo contratos accesorios de datos personales.

3. Por capacidad de influencia de hecho: Cuando en eventos diferentes de aquellos que pudieran encuadrarse en los casos anteriores, la persona está en condiciones de asumir las decisiones trascendentes como por ejemplo cuanto tiempo almacenar el dato, la modificación del mismo, etc. Es por ejemplo el caso de quien recolecta imágenes en sistemas de vigilancia, en cuyo caso no actúa por mandato legal ni contractual, de hecho ni siquiera media el consentimiento. Su actividad de Responsable surge justamente del hecho mismo de donde deriva su denominación.

De otra parte, el mismo artículo 3 de la LEPD, en el literal d, define al Encargado como la «Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento». En este caso, el factor diferenciador de esta categoría de sujeto de la relación de Hábeas Data será la circunstancia de la subordinación de este al Responsable. Así lo señala la misma jurisprudencia de la Corte Constitucional al decir:

> El criterio de delegación coincide con el término «por cuenta de» utilizado por el literal e), lo que da a entender una relación de subordinación del Encargado al Responsable, sin que ello implique que se exima de su responsabilidad frente al titular del dato (Sentencia C - 748 de 2011).

Hay que advertir que es posible que surja en la relación de tratamiento de Hábeas Data un subencargado, constituyéndolo la persona natural o jurídica que por cuenta del Encargado realice tratamiento de datos personales, figura esta que no ha sido contemplada en la legislación colombiana.

La Ley 1581 de 2012 ha definido las obligaciones a cumplir por parte de los Responsables, entre otras, en el artículo 17 cuyo texto advierte:

> Artículo 17. Deberes de los Responsables del Tratamiento.–Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:
>
> a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
>
> b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;
>
> c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
>
> d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
>
> e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
>
> f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que

previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

m) Informar a solicitud del Titular sobre el uso dado a sus datos;

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

En igual sentido el artículo 18 de la LEPD señaló las obligaciones de los Encargados, realizando una repetición de las obligaciones del Responsable, salvo por la referencia de las siguientes que fueron adicionadas:

g) Registrar en la base de datos la leyenda «reclamo en trámite» en la forma en que se regula en la presente ley;

h) Insertar en la base de datos la leyenda «información en discusión judicial» una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

Se considera que la redacción de los artículos 17 y 18 de la LEPD carecen de técnica legislativa pues, según el parágrafo final del artículo 18 de la LEPD, la concurrencia de la calidad de Responsable y En-

cargado en una misma persona, le genera el cumplimiento de las obligaciones previstas para cada uno, de donde se entendería, *a contrario sensu*, que de no ser así, las obligaciones señaladas para cada uno son exclusivas de cada uno de ellos. Sin embargo, tal interpretación no puede ser de recibo, toda vez que los literales g, h, i y j, del artículo 18 como obligaciones del Encargado y no incluidos en el artículo 17 de las obligaciones del Responsable, constituyen deberes que debe atender también este así no se les hubieran adjudicado expresamente. Y es muy obvio, pues en la práctica se evidencia que muchas veces las bases de datos se encuentran en poder tanto del uno como del otro, motivo por el cual a ambos ha de exigírsele el registro de las leyendas «reclamo en trámite» o «información en discusión judicial», al igual que los deberes de cumplimiento del principio de circulación restringida consagrados en el literal j o, con mayor razón, cumplir la orden de la Superintendencia de Industria y Comercio de abstenerse de circular información que esté siendo controvertida por el Titular. La redacción de los artículos 17 y 18 de la LEPD han de entenderse por tanto en el sentido que aquí se ha expresado, máxime cuando la Corte Constitucional ha advertido justamente sobre los mayores niveles de exigibilidad de cuidado y responsabilidad al Responsable que al Encargado, tal como se lee en sus propias palabras:

> Los responsables del tratamiento tienen mayores compromisos y deberes frente al titular del dato, pues son los llamados a garantizar en primer lugar el derecho fundamental al Hábeas Data, así como las condiciones de seguridad para impedir cualquier tratamiento ilícito del dato. La calidad de responsable igualmente impone un haz de responsabilidades, específicamente en lo que se refiere a la seguridad y a la confidencialidad de los datos sujetos a tratamiento (Sentencia C-748 de 2011).

Recuérdese, en todo caso, que la determinación precisa del rol de Responsable, Encargado o Subencargado, es de importancia por sobre todo al momento de pretenderse señalar responsabilidades frente al ejercicio de los derechos de los Titulares. No obstante, cuando no hubieren sido claramente definidos o de la operación misma del tratamiento no resulte fácil identificarlos, «**habrán de presumir la responsabilidad solidaria de todos**» (subrayado de origen) (Sentencia C-748 de 2011) cuando de responsabilidad civil contractual o extracontractual se trate.

Adicionalmente a la *responsabilidad civil*, el tratamiento de datos personales puede generar a los Responsables y Encargados *responsabilidad penal* que, para el caso colombiano, se pregona de las perso-

nas naturales y no de las jurídicas como ya se encuentra desarrollado en la normativa europea.

De otra parte, y sin necesidad de afectación de derechos del Titular, puede generarse *responsabilidad administrativa* para el Responsable y Encargado, cuando estos no logren demostrar ante la Superintendencia de Industria y Comercio –SIC– el cumplimiento de las obligaciones que la ley les ha impuesto. Para tal propósito, la SIC, por intermedio de la Delegada para la Protección de Datos Personales, con su Grupo De Investigaciones Administrativas, verifica que las políticas adoptadas por los Responsables y Encargados garanticen una estructura acorde al desarrollo organizacional, los mecanismos internos para el desarrollo de la política (herramientas de implementación, entrenamiento y programas de educación), así como los procesos de atención a Titulares *(artículo 2.2.2.25.6.2 del Decreto 1074 de 2015)* para lo cual, soportada en el artículo 2.2.2.25.6.1 *del Decreto 1074 de 2015*, verificará que las medidas adoptadas sean apropiadas y efectivas para garantizar los derechos de los Titulares, para lo cual se tendrán en cuenta los criterios que se muestran en la siguiente gráfica:

Figura 16. *Parámetros de* accountability *o responsabilidad demostrada (Basado en orientaciones de la SIC)*

«La definición de las medidas apropiadas y efectivas para garantizar los datos personales deberá revisarse en cada caso atendiendo a las características propias de cada organización.»

4.4.6 AUTORIDADES DE LOS DATOS PERSONALES Y FACULTAD SANCIONATORIA

El sexto elemento del Hábeas Data lo constituyen las autoridades que hacen eficaz la normativa que le regula. Para el caso colombiano, como se ha puesto de relieve durante todo el desarrollo del trabajo, la autoridad administrativa en materia de protección de datos personales es la Superintendencia de Industria y Comercio –SIC–, sin perjuicio de las funciones que le corresponden a los jueces en casos de asuntos civiles o penales que tengan que ver con violación de los mismos o la Procuraduría General de la Nación en cuanto corresponde a la responsabilidad de los funcionarios públicos por faltas a la ley (parágrafo del artículo 23 de la LEPD).

Dentro de las *competencias* que en el caso colombiano se han dado a la Autoridad de Protección de Datos (artículo 21 de la LEPD), que como se dijo es la SIC, se han señalado las siguientes:

a) Asegurar el cumplimiento de la ley, facultad que ejerce en la medida en que cumple las demás funciones que le han sido señaladas en su marco funcional.

b) Investigar las posibles violaciones al derecho de Hábeas Data asegurando el ejercicio de los derechos del titular y en desarrollo de las mismas imponer medidas cautelares (bloqueo temporal de datos) y finalmente imponer sanciones.

c) Divulgación pedagógica del tema.

d) Instruir sobre las medidas necesarias y efectivas a implementar en las organizaciones que tratan datos personales. Sobre esta función cabe señalar la expedición de la Guía de Responsabilidad Demostrada (Superintendencia de Industria y Comercio, 2015) que constituye el primer documento orientativo a las organizaciones que expide la SIC, en este caso sobre aplicación del principio de *accountability*.

e) Requerir a Responsables y Encargados para el cumplimiento de la ley.

f) «Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos». En relación con esta función ha de señalarse que hasta la fecha de elaboración del presente trabajo aún la SIC no ha definido los estándares con base en los cuales se determina la condición de país seguro o empresas seguras en el extranjero, frente a los eventos de transferencias internacionales.

g) «Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento». En relación con esta función, la Superintendencia de Industria y Comercio, a la fecha, como quedó dicho, ha aprobado ya el nuevo capítulo a incorporarse en la Circular Externa de la SIC, en desarrollo de lo ordenado por el Decreto 886 de 2014 reglamentario de la LEPD en relación con el Registro Nacional de Bases de Datos –RNBD.

h) Proponer cambios a la normativa.

i) «Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personajes».

En relación con las funciones de la SIC ha de señalarse que, conforme al artículo 23 de la LEPD, podrá imponer *sanciones* hasta de 2000 SMLMV, suspensiones temporales hasta por seis (6) meses, cierre de operaciones inmediato y definitivo.

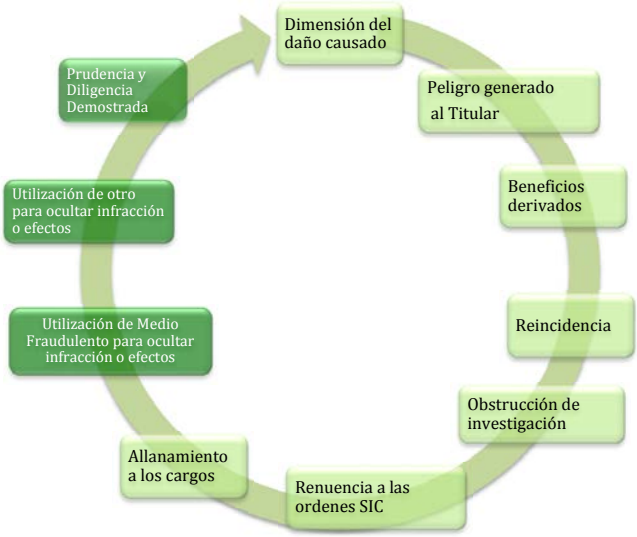


Figura 17. *Criterios de graduación de sanciones*

«Para efectos de la graduación de la sanción por violación de la ley 1581 de 2012, debe integrase esta norma con el CPACA artículo 50).»

Los *criterios para efecto de la graduación* de las sanciones habrán de consultar el sentido del artículo 24 ibídem en concordancia con el artículo 50 del CPACA, así:

a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;

b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;

c) La reincidencia en la comisión de la infracción;

d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;

e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;

f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar (artículo 24 de la LEPD).

g) Utilización de medios fraudulentos o utilización de persona interpuesta para ocultar la infracción u ocultar sus efectos.

h) Grado de prudencia y diligencia con que se hayan atendido los deberes o se hayan aplicado las normas legales pertinentes (artículo 50 del CPACA).

El *procedimiento sancionatorio,* reglado en principio como procedimiento especial en la LEPD, ha de integrarse con las normas del Código del Proceso Administrativo y de lo Contencioso Administrativo –CPACA– (Ley 1437 de 2011). En virtud de tal circunstancia, ha de tenerse que la *caducidad de la facultad sancionatoria* será de tres (3) años, es decir que, el acto administrativo que impone la sanción debe proferirse y en debida forma notificarse, dentro de dicho plazo. El mismo se debe contabilizar a partir de la conducta u omisión que dio origen a la misma o desde el día siguiente en que cesó la infracción o la ejecución (artículo 52 del CPACA). Adicionalmente, no es requisito que el acto administrativo quede en firme, es decir que cuando se interpongan recursos y estos se fallen fuera del tiempo de los tres años, habiéndose proferido y notificado la sanción dentro de dicho plazo, no operará la caducidad. Sin embargo, si los recursos interpuestos no han sido resueltos dentro del año siguiente a su «debida y oportuna interposición» (artículo 52 del CPACA), operará el

silencio administrativo positivo, es decir que se entenderá que se han resuelto a favor del recurrente.

TABLA 2. CESIÓN-COMUNICACIÓN Y TRANSMISIÓN DE DATOS

Concepto	Ley 15 de 1999 LOPD (España)	Ley 1581 de 2012 LEPD (Colombia)
Cesión de datos	Art. 3 literal i: «Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado»	No se identificó en la ley su uso ni en sus decretos reglamentarios
Comunicación de datos	Sinónimo de Cesión	Se utiliza en el artículo 4, y se infiere que se utiliza en el sentido de comunicar los datos a una persona distinta del titular.
Transmisión de datos	Solo se menciona una vez en toda la Ley 15 de 1999 (artículo 44, literal d) y se usa igualmente como sinónimo de comunicación.	La Ley nunca utiliza el término. Sin embargo, el Decreto 1074 de 2015, artículo 2.2.2.25.1.3, numeral 5 lo define como: «Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable». Es decir que involucra como remitente a un Responsable y como destinatario fuera o dentro del país, a un Encargado.

Cuando la decisión de sanción hubiere quedado en firme, ya por que no se interpusieron recursos o por que los interpuestos fueron fa-

llados negativamente al recurrente, la SIC tendrá solo 5 años para efectos de lograr la *efectividad de la sanción* interpuesta, término que se computará, ahí sí, a partir de la ejecutoria del acto administrativo que la impuso.

4.4.7 TRANSFERENCIA DE DATOS Y PAÍSES SEGUROS

Un séptimo elemento que integra el Hábeas Data corresponde a las operaciones de transferencia o transmisión de datos. Este es quizá uno de los elementos donde mayor imprecisión se ha generado por cuenta de la reglamentación nacional que, en su intento por seguir la normativa europea y en especial española, no ha generado una clara definición conceptual.

Para comprender lo afirmado, quepa en primer lugar identificar las dimensiones conceptuales de las expresiones cesión de datos, comunicación de datos, transferencia de datos, transmisión de datos, transferencia internacional y transmisión internacional, para lo cual se acude a la LOPD de España y a la Ley 1581 de 2012 junto con su Decreto Reglamentario 1074 de 2015 para el caso colombiano así:

TABLA 3. COMPARATIVO DE LA LOPD Y LA LEPD SOBRE TRANSMISIÓN DE DATOS

Concepto	**Ley 15 de 1999 LOPD (España)**	**Ley 1581 de 2012 LEPD (Colombia)**
Cesión de datos	Art. 3 literal i: «Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado».	No se identificó en la ley su uso ni en sus decretos reglamentarios
Comunicación de datos	Sinónimo de Cesión	Se utiliza en el artículo 4, y se infiere que se utiliza en el sentido de comunicar los datos a una persona distinta del titular.

Concepto	Ley 15 de 1999 LOPD (España)	Ley 1581 de 2012 LEPD (Colombia)
Transmisión de datos	Solo se menciona una vez en toda la Ley 15 de 1999 (artículo 44, literal d) y se usa igualmente como sinónimo de comunicación.	La ley nunca utiliza el término. Sin embargo, el Decreto 1074 de 2015, artículo 2.2.2.25.1.3, numeral 5 lo define como: «Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable». Es decir, que involucra como remitente a un Responsable y como destinatario fuera o dentro del país, a un Encargado.
Transferencia de datos	Referido en el artículo 33, 34, 44 y 49, se intuye, por su contenido y ubicación, que se utiliza también como sinónimo de comunicación.	Se utiliza en el artículo 21, 26 y 27 de la Ley, siempre en relación con la comunicación de datos a países diferentes a Colombia, sin que se tenga en cuenta la calidad de Responsable o Encargado del remitente o del destinatario. Sin embargo, el Decreto 1074 de 2015 la define como: «La transferencia de datos tiene lugar cuando el Responsable o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país». Es decir que involucra como remitente a un Responsable o un Encargado y como destinatario fuera del país, a un Responsable.
Transmisión internacional de datos	Nunca se usa esta expresión en la ley española.	La ley no utiliza nunca el término. Sin embargo, el Decreto 1074 de 2015, en los artículos 2.2.2.25.5.1 y 2.2.2.25.5.2, utiliza el término referido para describir un tipo de comunicación que involucra como remitente a un Responsable y como destinatario fuera del país, a un Encargado.

Concepto	Ley 15 de 1999 LOPD (España)	Ley 1581 de 2012 LEPD (Colombia)
Transferencia internacional de datos	Según el artículo 34 y 44, es usado como sinónimo de comunicación pero efectuada desde un país (España, para el caso) hacia otros países diferentes.	La ley no habla de transferencia internacional, pues pareciera un pleonasmo, como quiera que siempre que se refiere a Transferencia lo hace en relación con operaciones internacionales. Cuando utiliza la expresión lo hace para involucrar como remitente en Colombia a un destinatario fuera del país, sin atención a si se trata de Responsable o Encargado alguna de las partes de la operación. Sin embargo, aunque el Decreto 1074 de 2015 no usa la expresión Transferencia internacional del artículo 2.2.2.25.1.3, numeral 4, se infiere que la misma involucra como remitente a un Responsable o un Encargado y como destinatario fuera del país, a un Responsable.

Del anterior cuadro se extraen las siguientes observaciones: para el caso colombiano, las expresiones comunicación y cesión de datos, pueden ser usadas como sinónimos para referir, como lo hace la LOPD, a «toda revelación de datos realizada a una persona distinta del interesado». Por otra parte, en Colombia la transferencia y la transmisión, tanto nacionales como internacionales, son, según la normativa, formas de cesión o comunicación de datos personales, diferentes la una de la otra en razón de la calidad de Responsable o Encargado del remitente del dato o del destinatario del mismo, es decir que se adoptó un criterio subjetivo para diferenciarlas, caracterización que de suyo le es extraña a la fuente del trasplante.

Esta «creativa» categorización diferenciadora entre transmisión y transferencia, al momento de dar aplicación de las disposiciones, en tratándose de operaciones transfronterizas, genera incongruencias frente a los principios que regulan los datos personales, lo que hace sugerir su revisión legislativa o jurisprudencial. Para evidenciar lo afirmado resulta pertinente desagregar los eventos reglados, las orientaciones y exigencias para su ejecución conforme a la ley, lo mismo que aquellos eventos que han quedado por fuera de reglamentación, tal como se muestra en los siguientes cuadros.

TABLA 4. EVENTOS DE INTERCAMBIO INTERNACIONAL DE DATOS REGULADOS

Eventos regulados			
Remitente desde Colombia	**Destinatario fuera del país**	**Denominación de la operación**	**Requisitos legales**
Responsable	A otro responsable	Transferencia internacional de datos	Solo podrá realizarse a países con niveles adecuados de protección, según los estándares fijados por la SIC para tal propósito (artículo 26 de la LEPD). En el evento en que no sean países seguros, se requerirá declaración de conformidad de parte de la sic (artículo 26 de la LEPD). Excepto que: 1. Se cuente con autorización del titular, 2. Se trate de acciones ejecutadas en razón de tratados internacionales, 3. Se realice por motivos de salud o higiene pública (ibídem) y, 4. Se trate de la salvaguardia del interés público.
Encargado	A responsable		
Responsable	A un encargado	Transmisión internacional de datos	No se exige que sea a países con niveles adecuados de protección. No se exige autorización del titular pues, ni siquiera requiere ser informada a aquel cuando está de por medio un contrato de transmisión de datos personales (artículo 24, numeral 2, en concordancia con el 25) entre el responsable y el encargado.

La anterior tabla permite afirmar que dentro de la normativa nacional existe un vacío de reglamentación frente a eventos de movilización transfronteriza con Colombia que, justamente en razón de la diferenciación creada por la norma entre transferencia y transmisión, no son susceptible de encuadrarse en tales tipologías, impidiendo por tanto la definición de las obligaciones legales requeridas para el adecuado desarrollo de tales propósitos. Este es el caso, por ejemplo, de todas las operaciones de importación de datos desde otros países sobre el cual la norma ha guardado silencio, al igual que los eventos de exportación de datos que se describen en la siguiente figura.

TABLA 5. EVENTOS DE INTERCAMBIO INTERNACIONAL DE DATOS NO REGULADOS

Eventos no regulados		
Todas las operaciones de importación de datos provenientes del extranjero		
Otros eventos no regulados		
Remitente desde colombia	**Destino fuera del país**	**Categoría de la operación**
De Responsable	Al mismo Responsable	No está contemplado, aun cuando, siguiendo la línea del Decreto 1074 de 2015, se podría asimilar a Transferencia internacional de datos
De Encargado	Al mismo Encargado	No está contemplado y no hay elementos que permitan asimilarlo a una categoría específica
De Encargado	A otro Encargado (Subencargado)	No está contemplado y no hay elementos que permitan asimilarlo a una categoría específica

Por lo expuesto, ha de decirse que el proceso de trasplante normativo, tal vez por el propósito de tropicalización de las disposiciones incorporadas, ha resultado, en este aspecto, un tanto incompleto cuando no confuso.

Otro aspecto que ha incorporado la normativa en lo que a transferencia de datos refiere, lo constituye la prohibición de transferir datos personales a países que no brinden «niveles adecuados de protección de datos», para lo cual se delegó en cabeza de la SIC fijar los estándares que los definan, no pudiendo ser inferiores a las exigencias de la normativa existente.

Para el momento del desarrollo del presente trabajo aún la autoridad colombiana no había expedido la reglamentación correspondiente. No obstante, la Corte Constitucional, al revisar la constitucionalidad de la LEPD, en torno a la definición de país seguro, basándose para tal fin en las expresiones del Grupo de Trabajo del artículo 29 –GT29– creado por Directiva 95/46/CE como órgano consultivo integrado por las Autoridades de Protección de Datos de los países de la UE junto con el Supervisor Europeo de PD y la Comisión Europea, señaló como identificación de país seguro aquel que

> cuenta con los elementos o estándares de garantía necesarios para garantizar un nivel adecuado de protección de datos personales, si su legisla-

> ción cuenta; con unos **principios,** que abarquen las obligaciones y derechos de las partes (titular del dato, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos de datos personales), y de los datos (calidad del dato, seguridad técnica) y; con un **procedimiento** de protección de datos que involucre mecanismos y autoridades que efectivicen la protección de la información. De lo anterior se deriva que el país al que se transfiera los datos, no podrá proporcionar un nivel de protección inferior al contemplado en este cuerpo normativo que es objeto de estudio (Sentencia C-748 de 2011).

Es decir que, para considerarse un país seguro, habrá de identificarse la existencia de los siguientes elementos:

- Normativa que regule integralmente la materia de protección de datos personales
- Autoridad de protección de datos
- Procedimientos para acudir a la autoridad para hacer valer la normativa.

En tal sentido, resulta oportuno para las organizaciones públicas y privadas que se ven impelidas a realizar operaciones de «transferencia o transmisión» de datos desde Colombia al extranjero (cesiones de datos, contratos de servicios de alojamiento en web o contratos de *hosting,* por ejemplo*)*, en tanto se resuelven los aspectos pendientes de reglamentación por parte de la SIC, tener en cuenta los elementos advertidos y para identificar los países con normativa de protección de datos, consultar el apartado *«2.2. Diáspora Jurídica»*, del presente trabajo. Por otra parte, a efectos de identificar los países que ya cuentan con una autoridad de protección de datos personales, se sugiere consultar a la Agencia Española de Protección de Datos Personales (AGPD, 2013), quien ha identificado como tales a los siguientes:

> En Europa: Albania, Alemania, Andorra, Austria, Bélgica, Bosnia y Herzegovina, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Ex República Yugoslava de Macedonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Moldavia, Mónaco, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumanía, Serbia, Suecia y Suiza.
>
> En África: Burkina, Faso, Marruecos, Mauricio, Senegal y Túnez.
>
> En América: Argentina, Canadá, Colombia, Costa Rica, EE. UU., México, Perú y Uruguay.
>
> En Asia: Hong Kong, Israel y Corea del Sur.
>
> Oceanía: Australia Nueva Zelanda

Como puede observarse, los Estados Unidos de Norteamérica, país que ostenta la calidad de principal socio comercial de Colombia y por tanto destino permanente de intercambio de datos personales, no está referido dentro de los países con autoridad de protección de datos personales, de donde se deriva que, conforme a las normas nacionales colombianas no constituye un país con niveles adecuados para efectos de operaciones transfronterizas.

Respecto de la forma como ha sido abordado el tema la protección de datos personales en dicho país, cabe traer a referencia lo expresado por el Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos de la OEA quienes manifestaron a tal propósito que:

> En Estados Unidos, el derecho a la privacidad, a diferencia del enfoque europeo, protege solo contra la intrusión del gobierno federal en los asuntos privados de las personas. Por ende, la legislación específica sobre la cuestión de la protección de los datos personales se limita a los datos tratados o custodiados por el gobierno federal. Fuera de unas pocas leyes que tratan de la información personal financiera y médica, Estados Unidos no cuenta con una legislación que rija el procesamiento de datos personales por entidades privadas. Por el contrario, el sistema de ese país prevé la autorregulación por parte de los sectores económicos en materia de datos personales manejados por entidades privadas. En tal sentido, los sectores de la actividad privada de Estados Unidos están básicamente autorregulados, incluida la mayoría de las empresas privadas, las actividades de búsqueda de datos, los depósitos de datos personales y los sitios de redes sociales de Internet, entre otros. (…) Además, el hecho de que la legislación estadounidense se centre exclusivamente en la protección de la información de las personas que procesa el gobierno federal, no queda claro cuál es el nivel de protección asignado a los datos personales procesados por entidades privadas en Estados Unidos y, luego, transferidos a otro país (Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos, 2011).

Esta circunstancia fue la que produjo que la Unión Europea, desde 1999 iniciara negociaciones con el gobierno de Estados Unidos de Norte América, por cuanto que «La protección de la intimidad y de los datos en Estados Unidos se enmarca en un entramado de regulación sectorial, tanto a nivel federal como estatal, que se combina con la autorregulación industrial» (Portalweb AGPD, 2001).

Tal circunstancia, llevó a celebrar el Acuerdo de Puerto Seguro que

> consta de siete principios básicos, referidos a la notificación (información a los afectados), opción (posibilidad de oposición de los afectados), trans-

> ferencia ulterior a terceras empresas, seguridad, integridad de los datos (principios de finalidad y proporcionalidad), derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados). Dichos principios son, como se indicó, complementados con las «preguntas más frecuentes», básicamente referidas a tipos específicos de datos o tratamientos (Portalweb AGPD, 2001).

A partir de dicho acuerdo, los Estados Unidos, conforme a la LEPD en concordancia con el Decreto Real 1720 de 2007, ha sido considerado por la Agencia Española de Protección de Datos –AGPD– como país seguro, siempre y cuando se trate de las entidades adheridas al Acuerdo de Puerto Seguro (Safeharbor) y cuya identificación puede ser consultada en el enlace https://safeharbor.export.gov/list.aspx.

No obstante, la existencia del *Acuerdo Safeharbor*, en el caso de Colombia, el envío de datos personales a Estados Unidos de Norteamérica o a los demás países que sean considerados como que no ofrecen niveles adecuados de protección de datos, para el momento del presente trabajo, solo será posible previa «declaración de conformidad» por parte de la SIC, para lo cual se apoyará en la información que considere necesaria para evaluar la seguridad de la operación. A este respecto es importante señalar que, habida consideración de los volúmenes de actividad comercial con los Estados Unidos de Norteamérica, probablemente, de forma inconsciente, muchas organizaciones están realizando operaciones de transferencia internacional hacia ese destino en clara violación del ordenamiento jurídico nacional. Este criterio expuesto coincide con el del Tribunal de Justicia Europeo que el día 7 de octubre de 2015, mediante sentencia de la Gran Sala, declaró inválida la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000 [TRIBUNAL DE JUSTICIA (Gran Sala), 2015], que reconocía el nivel adecuado de protección del Puerto Seguro como mecanismo de reconocimiento de destino seguro para el envío de datos a los Estados Unidos de Norteamérica. Dentro de las argumentaciones dadas por el alto tribunal se tuvo que: «(...) al valorar el nivel de protección ofrecido por un tercer país la Comisión está obligada a apreciar el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales de éste, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender esa institución a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país, conforme al artículo 25, apartado 2, de

la Directiva 95/46». Esto significa que el mecanismo jurídico que Europa y EEUU habían acordado desde el año 2000, para facilitar el intercambio transfronterizo de datos, se ha quedado sin validez jurídica, dejando en el limbo miles de transacciones diarias de información que deben ser inmediatamente revisadas por las autoridades de protección de datos de los países de la unión europea. Así mismo constituye un campanazo para la Superintendencia de Industria y Comercio en Colombia que ha venido siempre siguiendo de cerca las orientaciones europeas y en especial las de la Agencia Española de Protección de Datos Personales.

4.4.8 CADUCIDAD DEL DATO

Finalmente, un elemento adicional del Hábeas Data lo constituye la caducidad del dato, esto es el tiempo a partir del cual el Responsable o el Encargado de un dato recolectado deberá suprimirlo por mandato legal o por solicitud del titular del mismo. El Decreto 1074 de 2015 en su artículo 2.2.2.25.2.8 advirtió el principio general según el cual los datos solo pueden ser tratados «durante el tiempo que sea razonable y necesario» y, cumplida o agotada la finalidad para lo cual fue recolectado, surge la obligación a los Responsables y Encargados de suprimirlos. Sin embargo, la ley consagró una excepción que corresponde a aquellos casos en que por razón de la ley o de un contrato se imponga su conservación.

Pero, ¿qué es plazo razonable? Al respecto ha dicho la Corte Constitucional que el término de caducidad «debe entenderse como un plazo prudencial para evitar un ejercicio abusivo del derecho a la información» (SU-082 de 1995), de hecho, incluso ha llegado a advertir que la figura de la caducidad está íntimamente ligada al derecho al olvido que, igual que aplica a la información financiera negativa, puede extenderse a

> otras actividades, que se haya recogido «en bancos de datos y en archivos de entidades públicas y privadas», como lo contempla el Art. 15 superior, por existir las mismas razones y porque dicha disposición no contempla excepciones (Sentencia C-1066 de 2002).

Por ello, en relación con el término de caducidad hay que decirse que no existe una única normativa que lo regule y, por el contrario, hay que abordarse el tema según la naturaleza de la información que

reportan lo datos (información financiera, información de antecedentes penales, información médica, etc.) a fin de definir en cada caso el término a aplicar, tal como se pasa a señalar.

A continuación, se presentan algunos de los eventos más comunes de operaciones ejecutadas al interior de las organizaciones y para las cuales la ley ha definido tiempo de caducidad del dato.

4.4.8.1 Caducidad de datos personales asociados a información financiera

En tratándose de información financiera la regla de caducidad posee varios regímenes y subreglas según las circunstancias fácticas así:

Régimen transitorio de caducidad

- Subregla 1.ª

Se aplica en favor de los Titulares de la información negativa que, a 31 de diciembre de 2008 fecha de entrada en vigencia de la Ley 1266 de 2008, estando al día en las obligaciones reportadas, hubieren permanecido en los bancos de datos por lo menos un año contado a partir de la cancelación de las obligaciones. En igual sentido operará en favor de aquellos que, estando al día al momento de la entrada en vigencia la ley, los datos negativos hubieren estado reportados por un tiempo inferior al año, caso en el cual la caducidad operará una vez cumplido dicho plazo. En uno y otro caso, será deber de la Fuente y del Operador de la Información de manera oficiosa, o en defecto de ello a solicitud del interesado, la supresión de los datos por parte de la entidad en los términos del artículo 21 de la Ley 1266 de 2008.

- Subregla 2.ª

Se aplicará en favor de quienes hubieren cancelado dentro de los seis (6) meses siguientes al 31 de diciembre de 2008 sus obligaciones vencidas, en cuyo caso el término de caducidad será de 1 año a partir de efectuado el pago (Ley 1266 de 2008).

Régimen de caducidad general

Se aplicará a favor de aquellos Titulares de información negativa no incluidos en las circunstancias anteriores, en cuyo caso el término

de caducidad operará, por regla general, en cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea pagada la obligación vencida, conforme al artículo 13 de la Ley 1266 de 2008.

No obstante esta regla general, la Corte Constitucional ha considerado este término de 4 años desproporcionado en ciertos casos y por ello ha establecido las siguientes subreglas:

> (**i**) la caducidad del dato financiero, en caso de que la mora haya ocurrido en un lapso inferior a dos años, no podrá exceder el duplo de la mora, (**ii**) si el titular de la obligación cancela las cuotas o el total de la obligación vencida en un lapso que supera los dos años de mora, el término de caducidad será de cuatro años contados a partir de la fecha en que este cumple con el pago de su obligación y, (**iii**) tratándose de obligaciones insolutas, el término de caducidad del reporte negativo también será de cuatro años, contado a partir de que la obligación se extinga por cualquier modo (T-658 de 2011 en concordancia con la C-1011 de 2008).

A estas subreglas ha de sumarse que las mismas aplican siempre que *durante dichos términos* «no se hayan reportado nuevos incumplimientos del mismo deudor, en relación con otras obligaciones» (SU-082 de 1995).

Regímenes especiales.

1. Caducidad de datos asociados a obligaciones canceladas en proceso ejecutivo:

Por otra parte, sobre la caducidad de los datos financieros en los eventos en que el pago de la obligación se produce en proceso ejecutivo, la Corte Constitucional ha dicho que

> es razonable que el dato (…) tenga un término de caducidad, que podría ser el de cinco (5) años, que es el mismo fijado para la prescripción de la pena, cuando se trata de delitos que no tienen señalada pena privativa de la libertad, en el Código Penal (...) (SU-082 de 1995).

2. Caducidad de datos asociados a obligaciones refinanciadas en crédito para vivienda:

Para el caso de Titulares de créditos de vivienda individual a largo plazo que hubieren sido objeto de reestructuración en los términos del artículo 42 de la Ley 546 de 1999, la cual operará «una vez haya cumplido puntualmente con el pago de las tres primeras cuotas de la

obligación reestructurada, tal como lo indica el artículo 52 Ley 546 de 1999 en los siguientes términos:

> **Artículo 52.** Registro **en centrales de riesgo.**–Los deudores de los créditos de vivienda individual a largo plazo que reestructuren sus créditos hipotecarios en los términos previstos en el artículo 42 de la presente ley, tendrán derecho a exigir que sus nombres se retiren como deudores morosos de las centrales de riesgo, una vez hayan cumplido puntualmente con el pago de las tres primeras cuotas de la obligación reestructurada. Los deudores hipotecarios de viviendas entregadas en dación en pago con posterioridad al 1.º de enero de 1997, tendrán derecho a que las entidades financieras los declaren a paz y salvo por el crédito respectivo y retiren sus nombres de las centrales de riesgo. Igualmente podrán beneficiarse de la opción de readquisición de vivienda establecida en el artículo 46 de la presente ley.

Esta medida excepcional se expresó como un paliativo a las graves e injustificadas afectaciones causadas a los deudores de los sistemas financieros, por sobre todo asociados a los modelos de crédito en Unidades de Poder Adquisitivo Constante –UPAC.

3. Caducidad de datos asociados a obligaciones de personas fallecidas.

En tratándose de los datos negativos de personas fallecidas, siguiendo el criterio esgrimido en la *Sentencia SU-458 de 2012* sobre la falta de utilidad y pérdida de vigor del interés protegido en la administración del dato, se entiende que la caducidad del dato es inmediata, pudiendo el causahabiente, previa acreditación del deceso del deudor, proceder a solicitar la cancelación de los datos negativos del causante. En tal sentido se ha expresado la Corte Constitucional en Sentencia *T-798 de 2007* donde afirmó:

> Una situación análoga se presenta en aquellos casos en los que, tras la muerte de una persona, su mal comportamiento financiero del pasado continúa siendo divulgado de manera indefinida a través de una base de datos o, por alguna eventualidad, se ingresa un reporte negativo sobre ella con posterioridad a su fallecimiento. La difusión de este tipo de información afecta el buen nombre y la memoria de quien aparece reportado como deudor incumplido después de su fallecimiento, pero igualmente lesiona la intimidad y la buena reputación de su familia, ya no solo por ver expuesta de manera indefinida una información negativa sobre uno de sus miembros, que ya no está ahí para defenderse de ella, sino en la medida en que tales datos puedan llegar a ser utilizados para elaborar el perfil de riesgo crediticio de los herederos de la persona que permanece o es reportada tras su muerte como deudora. Ello en tanto la información

> que se tenga sobre las deudas insolutas de una persona fallecida, puede influir en el juicio que se haga acerca de la solvencia económica y la capacidad de pago de quienes están llamados a sucederla en sus derechos y obligaciones (…) En consecuencia, las razones que llevaron a esta Corte a reconocer en la sentencia antes citada la legitimación a la madre de un fallecido para solicitar, a través de la tutela, la rectificación de la información que causaba agravio a la intimidad y honra de su hijo y a la de su familia, son válidas en esta ocasión para considerar legitimados a la cónyuge sobreviviente y a los herederos para conocer, actualizar y rectificar los datos que sobre su familiar fallecido reposa en una central de información financiera.

4.4.8.2 Caducidad de los datos personales asociados a sanciones disciplinarias, penales, contravencionales y fiscales

Hay que decirse respecto de los datos asociados a las sanciones de diversa naturaleza que, conforme al artículo 174 de la Ley 734 de 2002 que desarrolla el artículo 74 superior, el Estado lleva un registro unificado de antecedentes, en el cual hace constar las sanciones penales, disciplinarias, inhabilidades para contratar con el Estado, fallos de responsabilidad fiscal, perdidas de investidura y condenas contra servidores, ex servidores y particulares en ejercicio de funciones públicas. Tal registro lo lleva la Procuraduría General de la Nación a través de la División de Registro y Control y Correspondencia y como se desprende del artículo 6 literal d en concordancia con el 19 de la Ley 1712 de 2014, esta es información pública (recuérdese lo dicho en el apartado 3.4.2 sobre la diferencia entre información y dato) que puede ser clasificada como reservada. Surge entonces el interrogante sobre cuál ha de ser el tratamiento en materia de caducidad sobre los datos personales contenidos en dicho registro.

Sobre los datos contenidos en el referido registro unificado de antecedentes, en relación con la caducidad, la Corte Constitucional en Sentencia C-1066 de 2002, advirtió que, debe aplicarse también el derecho al olvido

> mediante el señalamiento de un término de caducidad razonable, de modo que los servidores públicos, los ex servidores públicos y los particulares que ejercen o han ejercido funciones públicas o tienen o han tenido la condición de contratistas estatales no queden sometidos por tiempo indefinido a los efectos negativos de dicho registro.

Por tal razón, a renglón seguido, consideró que la falta de un término de caducidad de información negativa consagrada en dicho registro viola el artículo 15 constitucional. Apoyado en tal criterio declaró:

> EXEQUIBLE el inciso final del Art. 174 de la Ley 734 de 2002, en el entendido de que solo se incluirán en las certificaciones de que trata dicha disposición las providencias ejecutoriadas dentro de los cinco (5) años anteriores a su expedición y, en todo caso, aquellas que se refieren a sanciones o inhabilidades que se encuentren vigentes en dicho momento (Sentencia C-1066 de 2002).

Cabe señalar sobre este proveído que, equivocadamente la jurisprudencia envía un mensaje según el cual la caducidad de los datos, es decir la obligación de suprimirlos oficiosamente o a solicitud de parte, está enmarcada por un tiempo de 5 años, lo cual bajo ningún criterio puede ser considerado, pues echaría por el traste toda la normativa que sobre inhabilidades intemporales constitucionales y legales (a las que se hará referencia adelante) ha establecido el régimen jurídico colombiano.

Confunde el alto tribunal el concepto de caducidad (ya tantas veces mencionado) con el de reserva de información. Debe entenderse que lo referido por la Corte al declarar la norma exequible, es al tiempo de reserva, que no de caducidad, de la información que se certifica como antecedentes (sanciones o inhabilidades que se encuentren vigentes provenientes de sentencias ejecutoriadas de los últimos cinco años).

De lo antes expuesto hay que decir por tanto que, la información que reposa en el registro único de antecedentes, por regla general, no está sometido a caducidad justamente por razón de la necesidad de la información requerida para efectos de la efectiva aplicación de las inhabilidades intemporales. No entenderlo en tal sentido sería desconocer entre otros, normas superiores y en especial el artículo 122 de la Constitución Política de Colombia y de paso dejaría sin fundamento el mismo artículo 174 de la Ley 734 de 2002 que ordena que «cuando se trate de nombramiento o posesión en cargos que exijan para su desempeño ausencia de antecedentes, se certificarán todas las anotaciones que figuren en el registro».

En buena hora la misma jurisprudencia logró corregir tan desacertada interpretación, y en SU-458 de 2012 claramente expresó que:

> (…) la supresión total de los antecedentes penales es imposible constitucional y legalmente. Ya lo vimos al referir el caso de las inhabilidades intemporales de carácter constitucional, las especiales funciones que en materia penal cumple la administración de esta información personal, así

> como sus usos legítimos en materia de inteligencia, ejecución de la ley y control migratorio. En estos casos, la finalidad de la administración de esta información es constitucional y su uso, para esas específicas finalidades, está protegido además por el propio régimen del Hábeas Data.

Sin embargo, a la regla general se le ha establecido una excepción construida por el mismo órgano constitucional y corresponde a los eventos en que la información almacenada en el referido registro unificado de antecedentes no provee utilidad alguna a los temas de las tantas veces mencionadas inhabilidades intemporales, en cuyo caso por perder conexidad con la finalidad del registro mismo

> deja de ser necesaria para la cumplida ejecución de las mismas, y no reporta una clara utilidad constitucional; por tanto, el interés protegido en su administración pierde vigor frente al interés del titular de tal información personal. En tales casos, la circulación indiscriminada de la información, desligada de fines constitucionales precisos, con el agravante de consistir en información negativa, y con el potencial que detenta para engendrar discriminación y limitaciones no orgánicas a las libertades, habilita al sujeto concernido para que en ejercicio de su derecho al Hábeas Data solicite la supresión relativa de la misma (Sentencia SU-458 de 2012).

En estos eventos, que constituye como se dijo excepción, la entidad estará obligada a suprimir los datos oficiosamente o a solicitud del titular pasados 5 años después de ejecutoriada la providencia penal, disciplinaria, fiscal o contravencional, siempre y cuando no se encuentren vigentes las mismas, en cuyo caso, terminada la vigencia de la sanción correspondiente y pasados los 5 años antes señalados, se cumple la caducidad.

4.4.9 CONSERVACIÓN DEL DATO

Íntimamente relacionado con la temática de la caducidad de los datos, como caras de una misma moneda, se encuentra los aspectos relacionados con la obligación legal que existe de conservar la información que contiene datos personales.

En tal sentido, así como la ley señala a los Responsables y Encargados la obligación de suprimir aquellos datos cuyo legítimo almacenamiento ya ha cesado, a su vez les advierte que en tratándose de ciertos datos, por el contrario, la obligación consiste en conservarlos mínimo por un tiempo determinado o en algunos casos debe conservarlos de manera indefinida.

Algunos de los eventos en que la obligación de conservación es intemporal, es decir de circunstancias que no tienen caducidad, son los siguientes:

4.4.9.1 Conservación intemporal de datos en interés general

Así como se ha establecido la caducidad, tal como se advirtió atrás, como una manifestación del derecho al olvido, así mismo, en sentido contrario, como manifestación del derecho a la información que le asiste a la ciudadanía y por sobre todo al Estado, se han establecido las denominadas inhabilidades intemporales tanto constitucionales como legales, respecto de las cuales los datos asociados a ellas no caducan. En torno a este aspecto, la jurisprudencia constitucional ha señalado que, cuando están de por medio datos asociados a circunstancias generadoras de inhabilidades intemporales constitucionales, no habrá caducidad de dicha información y por tanto la misma deberá tenerse permanentemente almacenada. Recuérdese que inhabilidad intemporal (constitucional o legal) justamente corresponde a aquella que ni el paso del tiempo puede eliminarla. La razón del establecimiento de ellas, como lo ha afirmado la Corte Constitucional, estriba en que:

> (i) (…) el objeto de las normas que las consagran no es castigar la conducta de la persona que resulta inhabilitada, sino asegurar la prevalencia del interés colectivo y la excelencia e idoneidad del servicio público, «mediante la certidumbre acerca de los antecedentes intachables de quien haya de prestarlo»; (ii) (…) están consagradas expresamente algunas inhabilidades intemporales, el legislador puede proceder en idéntica forma al establecer otras de carácter legal; (iii) (…) el legislador tiene un amplio margen de discrecionalidad a la hora de definir el régimen de inhabilidades.

Por lo tanto, los datos asociados a estas inhabilidades intemporales no podrán eliminarse en ningún tiempo, razón por la cual resulta importante su referencia, para cuyo efecto se mencionan, entre otras, las siguientes:

> 1. Declaratoria de inhabilidad permanente (administrativa o judicial) para inscribirse en el Registro Único de Proponentes –RUP– (que llevan las Cámaras de Comercio) y por tanto contratar con el Estado, por reincidencia en graves inconsistencias, conforme al artículo 6.º, numeral 6.3, parágrafo 5.º de la Ley 1150 de 2007. De esta normativa se deriva que, la información asociada a la sanción por cinco (5) años que pueden imponer las Cámaras de Comercio o la Jurisdicción Administrativa, ter-

mina siendo intemporal, pues de otra manera, resulta obvio, no podría cotejarse información para efectos de la reincidencia de que trata la misma ley. Al respecto puede consultarse la Sentencia C-1016 de 2012.

2. Inhabilidad para inscribirse como candidato a elección popularmente o ser elegido, ser designado servidor público o celebrar contratos con el Estado (personalmente o por interpuesta persona), por condena judicial por delitos contra el patrimonio del Estado y por delitos relacionados con «la pertenencia, promoción o financiación de grupos armados ilegales, delitos de lesa humanidad o por narcotráfico en Colombia o en el exterior» (artículo 122 de la C. P. de C.). Sobre esta inhabilidad puede consultarse la Sentencia C-652 de 2003.

3. Inhabilidad para inscribirse como candidato a elección popularmente o ser elegido, ser designado servidor público o celebrar contratos con el Estado (personalmente o por interpuesta persona) para el servidor público que diere ocasión a condena patrimonial contra el Estado por su conducta dolosa o gravemente culposa, calificada por sentencia ejecutoriada, y mientras no lo repare (C-652 de 2003).

4. Inhabilidades para ser notario por sanciones penales y disciplinarias conforme a las causales 4 a 7 del artículo 133 de la Ley 960 de 1970. Para mayor consulta la Sentencia C-373 de **2002.**

4.4.9.2 Conservación intemporal de datos en interés particular del titular

Sobre tan importante aspecto de los datos personales, la Corte Constitucional señaló en Sentencia T-926 de 2013 que:

> (…) los principios del Hábeas Data implican deberes constitucionales para las entidades que custodian y administran la información contenida en archivos y bases de datos. Así, dichas entidades deben observar una obligación general de seguridad y diligencia en la administración y conservación de los datos personales y una obligación específica de corregir e indemnizar los perjuicios causados por el mal manejo de la información. En este orden de ideas, debe resaltarse la importancia de que el acopio y la conservación de información se hagan con sujeción a los principios del Hábeas Data con el fin de garantizar su integridad y veracidad y así salvaguardar los demás derechos de los titulares de la información. Con frecuencia esta información es necesaria para acceder al goce efectivo de otros derechos fundamentales, toda vez que los datos personales, laborales, médicos, financieros y de otra índole que están contenidos en archivos y bases de datos, son la fuente de la información que se utiliza para evaluar el cumplimiento de los requisitos para el reconocimiento de derechos y prestaciones.

Teniendo en cuenta que no existe una regla general aplicable en todas las áreas respecto de la obligación de conservación de datos personales, resulta de valor tener presente algunas de ellas según la temática a que se vincula el dato que, conforme a la experiencia, están presentes en muchos de los procesos de las organizaciones, razón por la cual se refieren algunas de ellas así:

1. Datos asociados a los trabajadores: En relación con el término de conservación de los datos de los trabajadores no existe norma expresa que lo señale. Sin embargo la jurisprudencia constitucional *(Sentencia T-926 de 2013)* al derivar del artículo 57, numeral 7.º del CST la obligación intemporal del empleador de certificar, tiempo de servicio, salario devengado y la actividad cumplida, aún después de expirado el vínculo laboral, y a partir de ello reconocer el derecho imprescriptible para el trabajador, de solicitar la referida certificación, estableció como tiempo de conservación de los datos personales de los trabajadores el tiempo mismo de la existencia del empleador.

Esta obligación se extiende en general a toda la historia laboral del trabajador que entre otras contiene:

> toda la información, positiva o negativa, relacionada con su hoja de vida, desempeño en el ejercicio de funciones tales como reconocimientos, llamados de atención, suspensiones. Así mismo, la historia laboral contiene la información referente al tiempo laborado, las cotizaciones a la seguridad social, los periodos de vacaciones disfrutados o pendientes, el registro de sus cesantías, nombramientos, ascensos, traslados, retiros, incapacidades, comisiones de trabajo, entre otros datos indispensables para el goce de las prestaciones laborales que nuestro ordenamiento concede al trabajador (Sentencia T-718 de 2005).

Además, el empleador ha de saber que, en relación con la conservación de los datos de los trabajadores, deben asumirse ciertas medidas necesarias y efectivas para evitar causarles perjuicio con el uso inadecuado que de los mismos se realice, para lo cual ha de valorarse el tipo de dato y/o de información que lo contiene.

En la misma línea, en relación con los datos asociados a la salud de los trabajadores, que como es conocido son datos sensibles *(artículo 5 de la LEPD en concordancia con el artículo 2.2.2.25.1.3 del Decreto 1074 de 2015)* circunstancia que obliga a un especial tratamiento y conservación, han de tenerse como incorporados en el mismo tratamiento de conservación intemporal que se ha señalado arriba, pero respecto del tratamiento, ha de tenerse presente que, tal

como lo recomienda la OIT en el subpárrafo 1 del párrafo 14 de la Recomendación 171, deberán guardarse en «expedientes de salud personales y confidenciales», confiándosele exclusivamente a personal especializado para tal fin y a quien le asista la obligación de conservar el secreto médico (OIT, 1977).

2. Datos asociados a la seguridad social: Un universo normativo con implicaciones en el tema de datos personales, lo constituye la información de los trabajadores asociada a la seguridad social. Dada la naturaleza y objetivo de los datos vinculados a ella, al igual que la trascendencia que la misma implica en perspectiva de la dignidad humana para el Titular de dichos datos, se ha establecido la obligación de conservación de dicha información a cargo de las entidades del sistema de seguridad social. De hecho, se ha establecido la carga probatoria sobre la entidad que los poseen, tal como lo expresara la Corte Constitucional en la *Sentencia T-144 de 2013,* donde manifestó:

> Ahora bien, tratándose del registro de datos en la historia laboral de un afiliado al Sistema General de Seguridad Social, esta Corporación ha sostenido que las entidades que poseen dichos datos tiene una obligación de protección y diligencia que constituye también uno de los objetos del derecho fundamental al Hábeas Data. En efecto, dada la importancia que tiene la historia laboral de un trabajador para el reconocimiento de diferentes derechos y garantías laborales, es preciso que esta información sea cierta, precisa y fidedigna, ya que un error en la misma podría llevar al desconocimiento de ciertos derechos fundamentales.
>
> (…) Por ende, en caso de que la información de la historia laboral de un afiliado contenga inexactitudes y así lo advierta la entidad administradora de pensiones o se lo haga saber el propio afiliado, es deber de esta desplegar las actuaciones pertinentes que conduzcan a la corrección de cualquier información errónea o inexacta, pues de lo contrario se vulneraría el derecho al Hábeas Data al negarle al titular del derecho la posibilidad de que dichos datos sean corregidos o complementados, desconociendo por lo tanto la obligación de dichas entidades de registrar datos completos y veraces, que reflejen la realidad de la historia laboral del afiliado. Así, en sentencia T-855 de 2011 dijo esta Corporación:
>
> [a]l ser las entidades administradoras de pensiones las llamadas a la conservación, guarda y custodia de los documentos contentivos de la información correspondiente a la vinculación del afiliado al Sistema de Seguridad Social en Pensiones, no les es dable trasladarle al interesado las consecuencias negativas del deficiente cumplimiento de dichas obligaciones, es decir, de la pérdida, deterioro, desorganización o no sistematización de dicha información.

5. LA ISO/IEC 27001 EN COLOMBIA

5.1 MARCO HISTÓRICO SOCIO ECONÓMICO DE SURGIMIENTO

La historia del surgimiento de la norma NTC/ISO/IEC 27001:2013 está directamente asociada a la historia general del gobierno de las TI al interior de las organizaciones y en especial a la gestión de los riesgos de seguridad de la información.

La pérdida de la información y, dentro de ella los datos personales, su recuperación tardía o su restablecimiento incompleto, igual que el acceso a ellos por terceros no autorizados, se identificaron como riesgos organizacionales que podrían, si no poner fin a la existencia de la organización, si por lo menos ser causa de afectaciones económicas y/o políticas significativas. Se observó que, así como los riesgos asociados a la salud al interior de la empresa, por ejemplo, podían afectar a los trabajadores y de contera a la organización misma, también la inadecuada gestión de los riesgos de seguridad de la información podría poner en peligro la supervivencia de aquella. Baste imaginar lo que ocurriría a una entidad bancaria que perdiera, por alguna circunstancia, de manera irrecuperable la información de sus deudores, o una central hospitalaria cuyas historias clínicas se extravíen, o la entidad pública encargada de la recaudación de los tributos prediales a quien se le eliminara el registro de la propiedad inmueble de su localidad.

La realidad de riesgo organizacional por inadecuado tratamiento de la información, que se vio incrementada con creciente dependencia de los sistemas informáticos, fue despertando en diversos escenarios la necesidad de buscar la definición de estándares dirigidos a evaluar la seguridad de los sistemas y a definir las buenas prácticas que previnieran los riesgos que se derivaban de la gestión de la información.

Justamente el campo militar, como resulta lógico de entender, fue uno de los primeros en dedicar recursos y esfuerzos al propósito de establecer mecanismos de seguridad de la información. Por ello, en el año 1983, el Departamento de Defensa de los Estados Unidos de Norteamérica, produjo el denominado Trusted Computer System Evaluation Criteria –TCSEC– como un conjunto de estándares obligatorios

para la evaluación de la seguridad del tratamiento automatizado de datos (Hardware/firmware/software) en sus dependencias (Departament Of Defense –USA–, 1983). Por otra parte, en 1987, con miras a brindar seguridad de la información en el campo comercial e industrial, se creó el Centro de Seguridad de Computación Comercial (Commercial Computer Security Centre –CCSC–) como un área del Departamento de Industria y Comercio (Department of Trade and Industry –DTI–) del Reino Unido. A la naciente entidad se le encomendaron dos tareas esenciales en perspectiva de brindar apoyo a los proveedores de tecnología y con el propósito de proveer de orientación a los usuarios. La primera de ellas consistía en colaborar a los distribuidores de productos de seguridad tecnológica mediante el desarrollo de un conjunto de criterios de evaluación de la seguridad con capacidad de reconocimiento internacional, estableciendo así un *framework* para el logro de una certificación que reconociera la aplicación de aquellos. Tarea que fue cumplida a cabalidad dando origen al esquema ITSEC (Information Technology Security Evaluation Criteria). La segunda tarea consistió en generar para los usuarios de tecnologías un código de buenas prácticas de seguridad, dándose origen a lo que se denominó «Código de prácticas del Usuario» (Users Code of Practice), el cual fue publicado en 1989. Con el propósito de dar mayor fuerza valorativa, este código fue consolidado y perfeccionado por el Centro Nacional de Cómputo (National Computing Centre, NCC) inicialmente, y posteriormente validado por parte de un consorcio de la industria británica, buscando que el mismo lograra ser lo suficientemente amigable para el usuario. El resultado final se dio a conocer en 1993 como un documento guía de la British Standard Institution –BSI–, bajo el código de práctica PD0003, código de buenas prácticas para la gestión de la seguridad de la información. Luego de un periodo de consulta pública, esta norma fue relanzada como el Estándar Británico BS7799:1995, que, transformado en el año 1999, se dio a conocer como el BS7799:1999 (K. S. Tong & T. T. Wong, 2008, pp. 5-6). Su primera parte se convirtió, mediante mecanismo de «Fast Track» (trámite simplificado) (Mochal, 2006), en estándar de la International Organization for Standardization –ISO– en asocio con International Electrotechnical Commission –IEC–, dando así nacimiento a la ISO/IEC 17799:2000 el primero de diciembre de 2000 (Gamma SSL, 2014). Posteriormente esta norma se convirtió en la ISO/IEC 17799:2005, antecedente de la ISO/IEC 27001 cuya última versión se ha dado a cono-

cer en el año 2013. Es decir, esta es una norma que nació esencialmente en el seno de las organizaciones empresariales y con la finalidad especial de gestionar la implementación de sistemas de seguridad de la información operada por aquellas, razón que, sumadas a otras más que adelante se expresarán, fue tomada como base para el desarrollo del trabajo que en este escrito se presenta.

Como se refleja en el rápido desarrollo de la ISO/IEC 27001, la preocupación por la seguridad de la información fue en aumento. Para los gobiernos, por ejemplo, terminó convertido en un problema de seguridad estratégica, que año tras año ha demandado inversiones multimillonarias. A este respecto, el periodista del Economista.es, Carlos Bueno, poniendo de presente la importancia que representa para los gobiernos la necesidad de proteger la información, expresaba que:

> Si el problema fuera menor, el Departamento de Defensa estadounidense no se gastaría este año 3.000 millones de dólares para este concepto, bajo el eufemismo de «investigación, desarrollo e innovación de nuevas tecnologías de uso militar». Tampoco el Gobierno francés desembolsaría 1.500 millones de euros para adquirir capacidades de ciberdefensa. Y, como no podía ser de otra manera, también en esto hay niveles y niveles: Estados Unidos, Israel, China, Rusia o Reino Unido están a la cabeza, porque supieron ver a tiempo –30 años atrás– la importancia de esta cuestión.
>
> En el caso de España, el Ministerio de Defensa creó a finales de 2013 el Mando Conjunto de Ciberdefensa, que, entre otros objetivos, está elaborando un listado de infraestructuras críticas que habría que proteger. «Sin embargo, a nivel de ciberdelincuencia, con ataques a empresas y particulares, España es un productor de *malware* de primer nivel, situado entre los diez o 15 primeros puestos del mundo (...) (Bueno, 2015).

Como era de esperarse, la sofisticación de las varias formas de crímenes cuyo objetivo ha sido la información, llegaron al ciberespacio de tal manera que la denominada infraestructura de interconexión de los estados (redes bancarias, sistemas de control de defensa, canales de comunicación de la prensa, etc.) se ha visto altamente expuesta. El Ministerio de Defensa de Colombia (Ministerio de la Defensa Nal., Dirección de Estudios Sectoriales, Dirección de Programas, 2009) por ejemplo, sobre el particular expresaba que:

> En los últimos años, han surgido múltiples amenazas en contra de la infraestructura interconectada. Esta es altamente vulnerable y si se atenta contra ella, puede llegar a paralizarse completamente un país. Las amenazas cibernéticas tienen una connotación sustancialmente diferente a la de otras amenazas a la seguridad nacional; dado que éstas pueden tener dife-

rentes objetivos (pueden ser realizadas por diferentes tipos de actores (crimen organizado, terroristas o Estados), su costo es mínimo y su trazabilidad es sumamente difícil.

Para comprender la gravedad del tema, cabe referir uno de los casos documentados más trascendente en la historia de la cibercriminalidad y que pone de relieve la dimensión a la cual puede escalarse el riesgo. Se trata de la primera ciberguerra en el planeta, ocurrida en el año 2007, a raíz de la decisión del gobierno de Estonia por derribar el Monumento de Tõnismäe o Monumento a los Libertadores de Tallin (ciudad capital), levantado por el gobierno Ruso en 1947 en honor a los soldados caídos en la segunda guerra mundial. Aun cuando no se ha podido demostrar que el ciberataque provino del gobierno Ruso, se ha inferido que estuvo asociado al conflicto con dicho país. Para efectos de observar su desenlace, se presenta la siguiente ilustración que describe lo ocurrido en cada uno de los días álgidos del ciberataque:

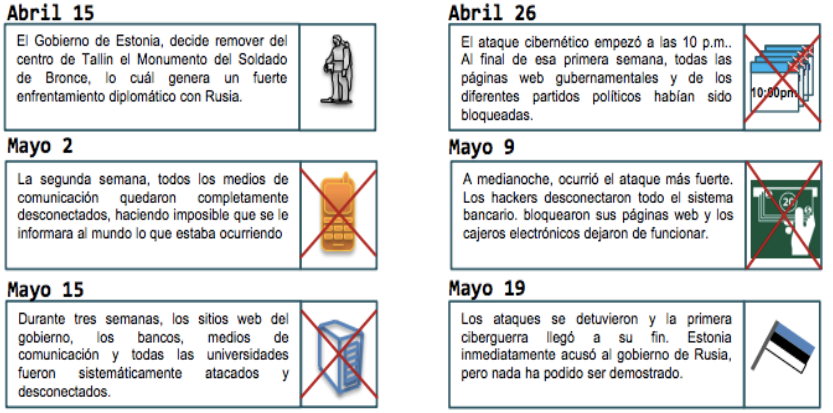
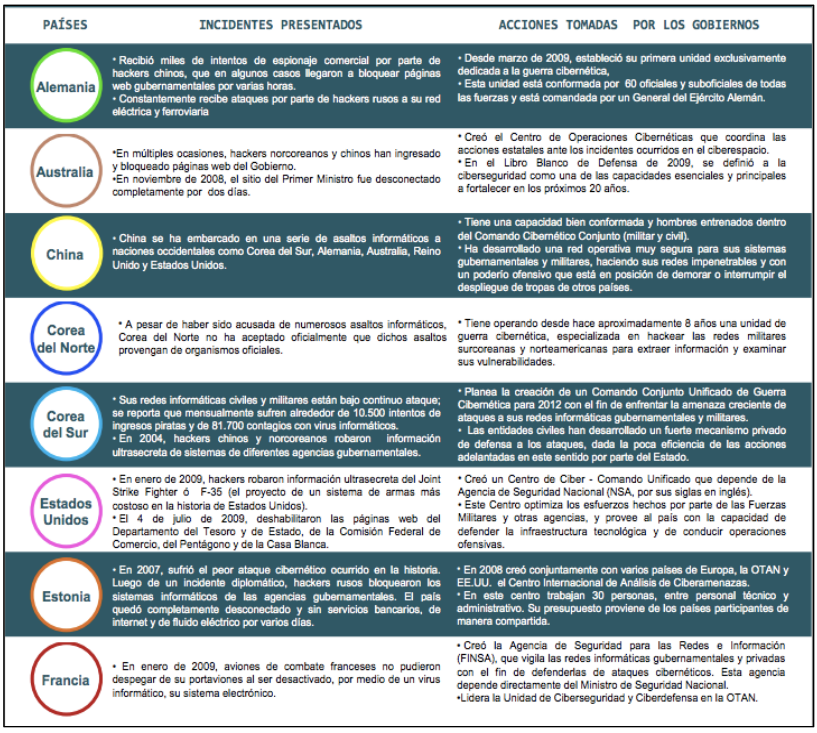


Figura 18. *Estonia 2007 – Caso documentado más grande de la historia de un ciberataque*

Fuente: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios% 20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

Estas amenazas, que sin lugar a dudas lo son de dimensiones globales, llevaron a que, en diferentes países, ante los ciberataques, se adoptaran estructuras de respuesta y prevención, como los equipos de respuesta a incidentes informáticos –CSIRT– (Computer Security Incident Response Team) o equipos de respuesta a emergencias infor-

máticas –CERT– (Computer Emergency Response Team). Estas denominaciones en algunas ocasiones han sido usadas como sinónimas en razón de los derechos de registro del nombre CERT, que efectuó la Universidad Carnegie Mellon. Con estas nuevas estructuras organizativas, se buscó contar con grupos dedicados a recibir informes reportados sobre incidentes o emergencias de seguridad para, previo análisis, brindar orientación sobre las acciones de respuesta a los mismo. Ejemplo de este tipo de acciones y de otras similares que fueron adoptadas por los Estados pueden apreciarse en la siguiente figura:



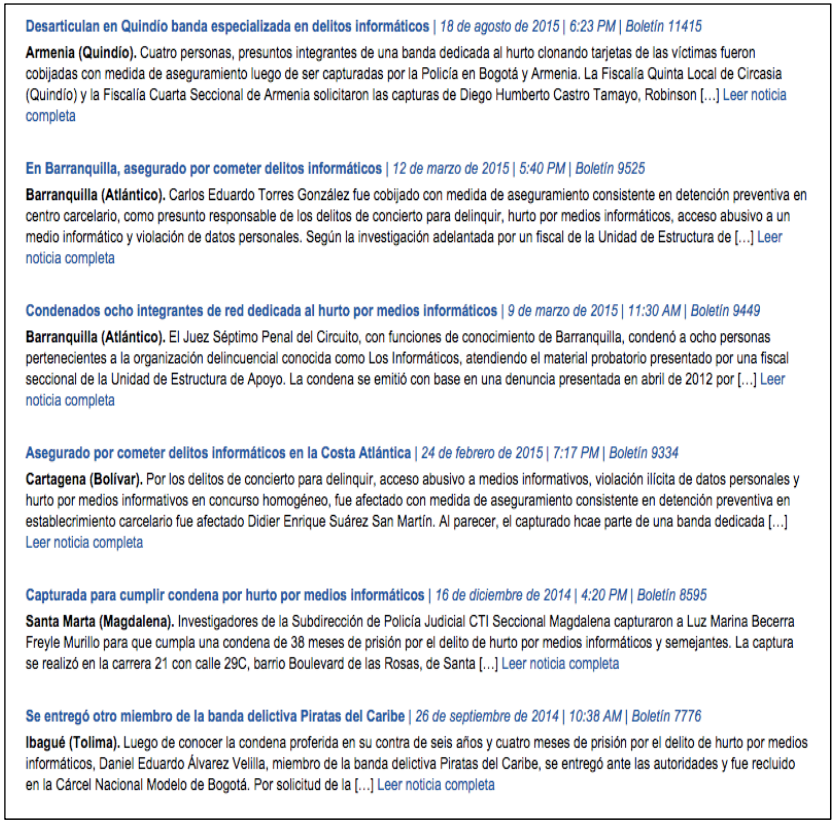
PAÍSES	INCIDENTES PRESENTADOS	ACCIONES TOMADAS POR LOS GOBIERNOS
Alemania	• Recibió miles de intentos de espionaje comercial por parte de hackers chinos, que en algunos casos llegaron a bloquear páginas web gubernamentales por varias horas. • Constantemente recibe ataques por parte de hackers rusos a su red eléctrica y ferroviaria	• Desde marzo de 2009, estableció su primera unidad exclusivamente dedicada a la guerra cibernética, • Esta unidad está conformada por 60 oficiales y suboficiales de todas las fuerzas y está comandada por un General del Ejército Alemán.
Australia	•En múltiples ocasiones, hackers norcoreanos y chinos han ingresado y bloqueado páginas web del Gobierno. •En noviembre de 2008, el sitio del Primer Ministro fue desconectado completamente por dos días.	• Creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio. • En el Libro Blanco de Defensa de 2009, se definió a la ciberseguridad como una de las capacidades esenciales y principales a fortalecer en los próximos 20 años.
China	• China se ha embarcado en una serie de asaltos informáticos a naciones occidentales como Corea del Sur, Alemania, Australia, Reino Unido y Estados Unidos.	• Tiene una capacidad bien conformada y hombres entrenados dentro del Comando Cibernético Conjunto (militar y civil). • Ha desarrollado una red operativa muy segura para sus sistemas gubernamentales y militares, haciendo sus redes impenetrables y con un poderío ofensivo que está en posición de demorar o interrumpir el despliegue de tropas de otros países.
Corea del Norte	• A pesar de haber sido acusada de numerosos asaltos informáticos, Corea del Norte no ha aceptado oficialmente que dichos asaltos provengan de organismos oficiales.	• Tiene operando desde hace aproximadamente 8 años una unidad de guerra cibernética, especializada en hackear las redes militares surcoreanas y norteamericanas para extraer información y examinar sus vulnerabilidades.
Corea del Sur	• Sus redes informáticas civiles y militares están bajo continuo ataque; se reporta que mensualmente sufren alrededor de 10.500 intentos de ingresos piratas y de 81.700 contagios con virus informáticos. • En 2004, hackers chinos y norcoreanos robaron información ultrasecreta de sistemas de diferentes agencias gubernamentales.	• Planea la creación de un Comando Conjunto Unificado de Guerra Cibernética para 2012 con el fin de enfrentar la amenaza creciente de ataques a sus redes informáticas gubernamentales y militares. • Las entidades civiles han desarrollado un fuerte mecanismo privado de defensa a los ataques, dada la poca eficiencia de las acciones adelantadas en este sentido por parte del Estado.
Estados Unidos	• En enero de 2009, hackers robaron información ultrasecreta del Joint Strike Fighter ó F-35 (el proyecto de un sistema de armas más costoso en la historia de Estados Unidos). • El 4 de julio de 2009, deshabilitaron las páginas web del Departamento del Tesoro y de Estado, de la Comisión Federal de Comercio, del Pentágono y de la Casa Blanca.	• Creó un Centro de Ciber - Comando Unificado que depende de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés). • Este Centro optimiza los esfuerzos hechos por parte de las Fuerzas Militares y otras agencias, y provee al país con la capacidad de defender la infraestructura tecnológica y de conducir operaciones ofensivas.
Estonia	• En 2007, sufrió el peor ataque cibernético ocurrido en la historia. Luego de un incidente diplomático, hackers rusos bloquearon los sistemas informáticos de las agencias gubernamentales. El país quedó completamente desconectado y sin servicios bancarios, de internet y de fluido eléctrico por varios días.	• En 2008 creó conjuntamente con varios países de Europa, la OTAN y EE.UU. el Centro Internacional de Análisis de Ciberamenazas. • En este centro trabajan 30 personas, entre personal técnico y administrativo. Su presupuesto proviene de los países participantes de manera compartida.
Francia	• En enero de 2009, aviones de combate franceses no pudieron despegar de su portaviones al ser desactivado, por medio de un virus informático, su sistema electrónico.	• Creó la Agencia de Seguridad para las Redes e Información (FINSA), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos. Esta agencia depende directamente del Ministro de Seguridad Nacional. •Lidera la Unidad de Ciberseguridad y Ciberdefensa en la OTAN.

Figura 19. *Registro de ataques de ciberseguridad y respuestas gubernamentales*

Fuente: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios %20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdF

En Colombia igualmente los ataques en materia de ciberseguridad no fueron extraños. Los ocurridos incluso llegaron a comprometer

instancias públicas y privadas, estimándose que del total de los ataques efectuados el 3% de ellos fueron dirigidos en contra del mismo gobierno nacional (Semana, 2015). De hecho, en el registro de los boletines de prensa de la máxima autoridad de investigación penal, esto es la Fiscalía General de la Nación, se tornó usual encontrar las referencias a este tipo de delitos, tal como lo muestra la imagen tomada de la página de dicha institución.



Desarticulan en Quindío banda especializada en delitos informáticos | *18 de agosto de 2015 | 6:23 PM | Boletín 11415*

Armenia (Quindío). Cuatro personas, presuntos integrantes de una banda dedicada al hurto clonando tarjetas de las víctimas fueron cobijadas con medida de aseguramiento luego de ser capturadas por la Policía en Bogotá y Armenia. La Fiscalía Quinta Local de Circasia (Quindío) y la Fiscalía Cuarta Seccional de Armenia solicitaron las capturas de Diego Humberto Castro Tamayo, Robinson […] Leer noticia completa

En Barranquilla, asegurado por cometer delitos informáticos | *12 de marzo de 2015 | 5:40 PM | Boletín 9525*

Barranquilla (Atlántico). Carlos Eduardo Torres González fue cobijado con medida de aseguramiento consistente en detención preventiva en centro carcelario, como presunto responsable de los delitos de concierto para delinquir, hurto por medios informáticos, acceso abusivo a un medio informático y violación de datos personales. Según la investigación adelantada por un fiscal de la Unidad de Estructura de […] Leer noticia completa

Condenados ocho integrantes de red dedicada al hurto por medios informáticos | *9 de marzo de 2015 | 11:30 AM | Boletín 9449*

Barranquilla (Atlántico). El Juez Séptimo Penal del Circuito, con funciones de conocimiento de Barranquilla, condenó a ocho personas pertenecientes a la organización delincuencial conocida como Los Informáticos, atendiendo el material probatorio presentado por una fiscal seccional de la Unidad de Estructura de Apoyo. La condena se emitió con base en una denuncia presentada en abril de 2012 por […] Leer noticia completa

Asegurado por cometer delitos informáticos en la Costa Atlántica | *24 de febrero de 2015 | 7:17 PM | Boletín 9334*

Cartagena (Bolívar). Por los delitos de concierto para delinquir, acceso abusivo a medios informativos, violación ilícita de datos personales y hurto por medios informativos en concurso homogéneo, fue afectado con medida de aseguramiento consistente en detención preventiva en establecrimiento carcelario fue afectado Didier Enrique Suárez San Martín. Al parecer, el capturado hcae parte de una banda dedicada […] Leer noticia completa

Capturada para cumplir condena por hurto por medios informáticos | *16 de diciembre de 2014 | 4:20 PM | Boletín 8595*

Santa Marta (Magdalena). Investigadores de la Subdirección de Policía Judicial CTI Seccional Magdalena capturaron a Luz Marina Becerra Freyle Murillo para que cumpla una condena de 38 meses de prisión por el delito de hurto por medios informáticos y semejantes. La captura se realizó en la carrera 21 con calle 29C, barrio Boulevard de las Rosas, de Santa […] Leer noticia completa

Se entregó otro miembro de la banda delictiva Piratas del Caribe | *26 de septiembre de 2014 | 10:38 AM | Boletín 7776*

Ibagué (Tolima). Luego de conocer la condena proferida en su contra de seis años y cuatro meses de prisión por el delito de hurto por medios informáticos, Daniel Eduardo Álvarez Velilla, miembro de la banda delictiva Piratas del Caribe, se entregó ante las autoridades y fue recluido en la Cárcel Nacional Modelo de Bogotá. Por solicitud de la […] Leer noticia completa

Figura 20. *Registro de noticias de la Fiscalía General de la Nación sobre delitos informáticos*

Fuente: http://www.fiscalia.gov.co/colombia/tag/delitos-informaticos/

El Gobierno Nacional de Colombia, ante las amenazas evidentes en el ciberespacio, y considerado este ámbito militarmente como el quinto domino de control (junto con el mar, el aire, la tierra y el espacio), llegó a

aprobar, a través del Consejo Nacional de Política Económica y Social, el documento Conpes 3701 del 14 de julio de 2011 con los lineamientos de la política para ciberseguridad y ciberdefensa, «orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país» (Consejo Nacional de Política Económica y Social de la República de Colombia, 2011). De hecho, con base en dicha decisión, y con el objetivo de «Implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional» (Consejo Nacional de Política Económica y Social de la República de Colombia, 2011, pág. 20) creó la Comisión Intersectorial como parte del esquema de ciberseguridad y ciberdefensa, conformada por el Presidente de la República, como cabeza de la misma, el Alto Asesor para la Seguridad Nacional, el Ministro de Defensa Nacional, el Ministro de Tecnologías de Información y Comunicaciones, el Director de Planeación Nacional y el Coordinador del ColCERT» (Consejo Nacional de Política Económica y Social de la República de Colombia, 2011, pág. 21), quienes actúan de la mano del Comando Conjunto Cibernético de las Fuerzas Militares (Ccoc) y el Centro Cibernético Policial (CCP), organismos estos últimos igualmente de reciente creación.

Figura 21. *Modelo de Coordinación*

Fuente: Ministerio de Defensa Nacional. Tomado del Conpes 3701 del 14 de julio de 2011.

Sumado a las acciones en el ámbito gubernamental para efectos de la gestión del riesgo de la información, en el sector privado se terminaron realizado significativas inversiones ante las afectaciones también multimillonarias. En informe presentado en junio de 2014 por la OEA (OEA, 2014), por ejemplo, se advirtió que, en América Latina, las pérdidas económicas asociadas con el cibercrimen, no obstante, son difíciles de cuantificar,

> (…) se estima que ascendieron a por lo menos USD 113,000 millones, suma suficiente para comprar un iPad a toda la población de México, Colombia, Chile y Perú. Solamente en Brasil, los costos de los delitos cibernéticos alcanzaron los USD 8,000 millones, seguidos por México con USD 3,000 millones y Colombia, con USD 464 millones. A nivel mundial, una de cada ocho violaciones de datos dieron como resultado la exposición de 10 millones de identidades; además, la cantidad de ataques dirigidos se incrementó. Al mismo tiempo, la actitud laxa de los usuarios finales respecto de las redes sociales, junto con la mayor adopción de dispositivos móviles condujo al aumento de estafas y generó mayores oportunidades para los ciberdelincuentes, en un momento en que el uso de las redes sociales en dispositivos móviles desempeña un papel preponderante cada vez mayor en la vida cotidiana, en especial en América Latina y el Caribe.

En México, por ejemplo, en el 2013 se estimó que cerca de 45 millones de personas fueron víctimas de algún tipo de ciberataque, ubicando al país en el tercer lugar en cibercrímenes en América Latina, según la investigación del académico Julio Téllez, del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México DF (Prensa Latina, Agencia Informativa Latinoamericana, LP, 2014).

De hecho, hacia el futuro, se calcula que para el 2019 los costes por brechas de seguridad asociados a datos serán de 2,1 billones de dólares y «Con más negocios e infraestructuras conectadas, la media del coste de una brecha de datos en 2020 superará los 150 millones de dólares» (CSO España-Computerworld, 2015).

La sumatoria de todas estas realidades descritas, tanto en el sector empresarial como en el gubernativo, obligaron a enfocar esfuerzos y recursos hacia el desarrollo de nuevas habilidades organizacionales asociadas a la seguridad de la información y por supuesto, de contera a la seguridad de los datos personales, generando una nueva mirada a la infraestructura de TI y propiciando la aparición de una especiali-

dad dentro de la gestión empresarial denominada el gobierno de las TI entendido éste último en términos de Muñoz & Ulloa como

> la estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos, por medio de agregar valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos (Muñoz Periñán & Ulloa Villegas, 2011).

El objetivo central del gobierno de las TI, como lo describe Dejan Kosutic (Kosutic, Ciberseguridad en 9 pasos, 2012, pág. 24), buscaba:

> la «preservación de la confidencialidad, integridad y disponibilidad de la información» (ISO/IEC 27001:2005), donde confidencialidad es «la propiedad de que la información no sea puesta a disposición de, o se divulgue a, individuos, entidades o procesos no autorizados», integridad es «la propiedad de mantener la exactitud y completitud de los activos» y disponibilidad es «la propiedad de ser accesibles y utilizables ante la demanda de una entidad autorizada».

Es decir que, en otros términos, con el gobierno de las TI, al interior de una organización, se pretendió buscar «(…) el uso eficiente de los recursos de TI para apoyar el cumplimiento de los objetivos del negocio» como lo refiere ISACA, citado por Helkyn Coello (Coello, 2009). Por ello, en la línea del pensamiento de Muñoz & Ulloa (Muñoz Periñán & Ulloa Villegas, 2011, pág. 29) igual que un buen gobierno corporativo era elemental para asegurar y alinear las decisiones claves de negocio, con la visión y estrategia de la compañía, también un buen gobierno de TI se convertiría en elemento crítico para asegurar que las decisiones de TI estuviesen alineadas a los objetivos de la compañía.

Por ello, el gobierno de las TI, que implicó un conjunto de labores agrupadas en cinco áreas, conforme lo describe el ITGI referido por Muños & Ulloa (Muñoz Periñán & Ulloa Villegas, 2011, págs. 29-30), esto es, Alineamiento estratégico, Entrega de valor, Medición del desempeño, Administración de recursos y Administración de riesgos, demandó una conciencia clara de la alta dirección sobre la importancia de la gestión de los riesgos y en general al interior de la organización de una definición precisa de los requerimientos en materia de cumplimiento interno y externo, una identificación de los riesgos significativos de la organización, la definición de roles y competencias asociados a los riesgos, es decir la implementación de un sistema de gestión de la nueva realidad.

La realidad del reto que se imponía para la gestión del riesgo seguridad de la información puede observarse de manera gráfica en la ilustración que Dejan Kosutic (Kosutic, Ciberseguridad en 9 pasos, 2012, pág. 26) utilizó para describir la relación entre ciberseguridad y seguridad de la información.

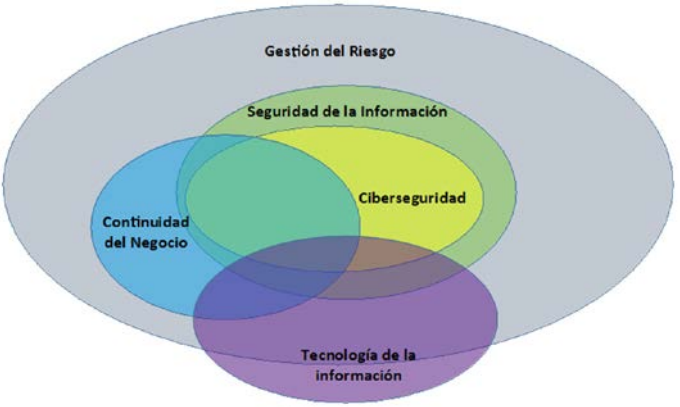


Figura 22. *Relación entre seguridad de la información y ciberseguridad*

Fuente: Ciberseguridad en 9 pasos, el manual para la ciberseguridad de la información del Gerente de Dejan Kosutic, 2012.

«Desde que se incorporaron las herramientas tecnológicas de información y comunicaciones, la gestión de los riesgos organizaciones incorporó en el área de la seguridad de la información tanto la ciberseguridad como la continuidad del negocio.»

Tal como se aprecia, el universo enorme de la gestión de los riesgos de una organización terminó involucrando, en el tema específico de la información, aspectos referidos a la ciberseguridad, continuidad del negocio, gestión de activos informáticos e incluso archivos análogos (físicos), constituyendo un reto enorme para la gerencia misma de las organizaciones.

Esta nueva demanda llevó al desarrollo permanente de nuevas herramientas, además de la TCSEC antes mencionada, como lo han sido: COBIT, publicado por ISACA (Information Systems Audit and Control Association); NIST SP 800, sobre seguridad de TI, realizada por el Instituto Nacional de Normas y Tecnología de los Estados Unidos; PCI DSS del Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC); ITIL de la Oficina Gubernamental de

Comercio (OGC) del Reino Unido; y BS 25999-2 para los Sistema de Gestión de la Continuidad del Negocio; o la NFPA 1600 de la Asociación Nacional de Protección contra Incendios de los Estados Unidos (Kosutic, Ciberseguridad en 9 pasos, 2012, págs. 46-51) y por su puesto junto a ellas la ISO/IEC 27001 al lado de toda la serie 27000.

5.2 MARCO REGULATORIO DE LA NORMA ISO/IEC 27001-2013

La norma ISO/IEC 27001, base de la NTC/ISO/IEC27001:2013, forma parte del universo de los estándares con reconocimiento internacional, dirigidos a unificar las calidades de los productos o servicios que se intercambian en el mercado.

La fuente institucional de la referida norma se radica en cabeza de dos organismos de normalización internacional. Por una parte, a la International Organization for Standardization, que por sus siglas debía denominarse IOS y no ISO, aun cuando se optó por esta denominación acogiendo la palabra griega *isos* que traduce igual, en una clara identificación con el propósito de dichos estándares. La ISO, integrada por los organismos nacionales de normalización de 159 países (normalmente reconocidos como tales por los gobiernos) (ISO, 2010, pág. 4),

> (…) identifica cuáles normas internacionales son requeridas por el comercio, los gobiernos y la sociedad; las desarrolla conjuntamente con los sectores que las van a utilizar; las adopta por medio de procedimientos transparentes basados en contribuciones nacionales proveniente de múltiples partes interesadas; y las ofrece para ser utilizadas a nivel mundial (ISO-ONUDI, 2010, pág. 1).

Y, por otra parte, de la mano de la ISO, como institución fuente de la norma 27001 la Comisión Electrotécnica Internacional –IEC– (por sus siglas en Ingles), organización internacional que agrupando 166 países (83 miembros y 83 afiliados) representados por sus correspondientes Comisiones Nacionales –CN–, se define como

> organización mundial líder que publica Normas Internacionales globalmente pertinentes para todas las tecnologías eléctricas, electrónicas y demás relacionadas, y respalda toda forma de evaluación de conformidad y administra Sistemas de EC (evaluación de la conformidad) de tercera parte» (IEC, 2015, p. 30).

Estos dos organismos de normalización internacional sumaron sus conocimientos para generar la denominada serie 27000 (salvo la ISO 27799:2012 referida a los SGSI en el sector sanitario), donde la columna vertebral está conformada por la ISO/IEC 27001:2013. Las demás son herramientas coadyuvantes (definiciones, guías, aplicativos sectoriales o temáticos) todas ellas dedicadas al tema de seguridad de la información –SI–, como puede apreciarse del rápido resumen que de cada una de las normas de la serie presenta el portal ISO27000.es (ISO27000.es, 2012) así:

> ISO/IEC 27000: (…) tercera edición de 14 de enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua.
>
> ISO/IEC 27001: (…) Revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI (…) Desde el 12 de noviembre de 2014, esta norma está publicada en España como UNE-ISO/IEC 27001:2014 y puede adquirirse online en AENOR. En 2015, se publicó un documento adicional de modificaciones (UNE-ISO/IEC 27001:2014/Cor 1:2015). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27001), Chile (NCh-ISO27001) o Uruguay (UNIT-ISO/IEC 27001). El original en inglés y la traducción al francés pueden adquirirse en iso.org.
>
> ISO/IEC 27002: Publicada desde el 1 de julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 (a la venta en AENOR). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002), Uruguay (UNIT-ISO/

IEC 27002) o Perú (como ISO 17799; descarga gratuita). Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de septiembre de 2013.

ISO/IEC 27003: Publicada el 01 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. En España, esta norma aún no está traducida, pero sí en Uruguay (UNIT-ISO/IEC 27003). El original en inglés puede adquirirse en iso.org. Actualmente en proceso de revisión para su actualización.

ISO/IEC 27004: Publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001. En España, esta norma aún no está traducida, sin embargo, sí lo está en Argentina (IRAM-ISO-IEC 27004) o Uruguay (UNIT-ISO/IEC 27004). El original en inglés puede adquirirse en iso.org. Actualmente en proceso de revisión para su actualización.

ISO/IEC 27005: Publicada en segunda edición el 1 de junio de 2011 (primera edición del 15 de junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000. El original en inglés puede adquirirse en iso.org. En España, esta norma no está traducida, sin embargo, sí lo está, para la versión de 2008, en países como México (NMX-I-041/05-NYCE), Chile(NCh-ISO27005), Uruguay (UNIT-ISO/IEC 27005) o Colombia (NTC-ISO-IEC 27005). Actualmente en proceso de revisión para su actualización.

ISO/IEC 27006: Publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos

específicos relacionados con ISO 27001:2005 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. El original en inglés puede adquirirse en iso.org. En España, esta norma no está traducida, sin embargo, sí lo está, para la versión de 2007, en México (NMX-I-041/06-NYCE) o Chile (NCh-ISO27001). Actualmente finalizando el proceso de revisión para una nueva versión.

ISO/IEC 27007: Publicada el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. En España, esta norma no está traducida. El original en inglés puede adquirirse en iso.org. Actualmente en proceso de revisión para su actualización.

ISO/IEC TR 27008: Publicada el 15 de octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI. En España, esta norma no está traducida. El original en inglés puede adquirirse en iso.org. Actualmente en proceso de revisión para su actualización.

ISO/IEC 27009: En estado de desarrollo. No certificable. Es una guía sobre el uso y aplicación de los principios de ISO/IEC 27001 para el sector servicios específicos en emisión de certificaciones acreditadas de tercera parte.

ISO/IEC 27010: Publicada el 20 de octubre de 2012. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto pública como privada, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones. Actualmente en proceso de revisión para su actualización.

ISO/IEC 27011: Publicada el 15 de diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002:2005. Está publicada también como norma ITU-T X.1051. En España, no está traducida. El original en inglés puede adquirirse en iso.org. Actualmente en proceso de revisión para su actualización.

ISO/IEC 27013: Publicada el 15 de octubre de 2012. Es una guía de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI). Actualmente finalizando el proceso de revisión para su actualización.

ISO/IEC 27014: Publicada el 23 de abril de 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información.

ISO/IEC TR 27015: Publicada el 23 de noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.

ISO/IEC TR 27016: Publicada el 20 de febrero de 2014. Es una guía de valoración de los aspectos financieros de la seguridad de la información.

ISO/IEC TS 27017: En fase de desarrollo, con publicación prevista en 2015. Consistirá en una guía de seguridad para Cloud Computing.

ISO/IEC 27018: Publicada el 29 de julio de 2014. Es un código de buenas prácticas en controles de protección de datos para servicios de computación en *cloud computing*.

ISO/IEC TR 27019: Publicada el 17 de julio de 2013. Guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía. Actualmente en proceso de revisión para su actualización.

ISO/IEC 27031: Publicada el 01 de marzo de 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777. En España, esta norma no está traducida. El original en inglés puede adquirirse eniso.org

ISO/IEC 27032: Publicada el 16 de julio de 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.

ISO/IEC 27033: Parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales (Publicada el 15 de diciembre de 2009); 27033-2, directrices de diseño e implementación de seguridad en redes (Publicada el 27 de julio de 2012); 27033-3, escenarios de referencia de redes (Publicada el 3 de diciembre de 2010); 27033-4, aseguramiento de las comunicaciones entre redes mediante *gateways* de seguridad (Publicada el 21 de febrero de 2014);

27033-5, aseguramiento de comunicaciones mediante VPNs (Publicada el 29 de julio de 2013); 27033-6, convergencia IP (en desarrollo); 27033-7, redes inalámbricas (en propuesta de desarrollo).

ISO/IEC 27034: Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 6 partes: 27034-1, conceptos generales (Publicada el 21 de noviembre de 2011); 27034-2, marco normativo de la organización (en desarrollo); 27034-3, proceso de gestión de seguridad en aplicaciones (en desarrollo); 27034-4, validación de la seguridad en aplicaciones (en desarrollo); 27034-5, estructura de datos y protocolos y controles de seguridad de aplicaciones (en desarrollo); 27034-6, guía de seguridad para aplicaciones de uso específico (en desarrollo).

ISO/IEC 27035: Publicada el 17 de agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información. Consta de 3 partes adicionales actualmente en fase de desarrollo.

ISO/IEC 27036: Guía en cuatro partes de seguridad en las relaciones con proveedores: 27036-1, visión general y conceptos (Publicada el 24 de marzo de 2014); 27036-2, requisitos comunes (Publicada el 27 de febrero de 2014); 27036-3, seguridad en la cadena de suministro TIC (Publicada el 08 de noviembre de 2013); 27036-4, seguridad en entornos de servicios Cloud (en desarrollo).

ISO/IEC 27037: Publicada el 15 de octubre de 2012. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

ISO/IEC 27038: Publicada el 13 de marzo de 2014. Es una guía de especificación para seguridad en la redacción digital.

ISO/IEC 27039: Publicada el 11 de febrero de 2015. Es una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).

ISO/IEC 27040: Publicada el 05 de enero de 2015. Es una guía para la seguridad en medios de almacenamiento.

ISO/IEC 27041: Publicada el 19 de junio de 2015. Es una guía para garantizar la idoneidad y adecuación de los métodos de investigación.

ISO/IEC 27042: Publicada el 19 de junio de 2015. Es una guía con directrices para el análisis e interpretación de las evidencias digitales.

ISO/IEC 27043: Publicada el 04 de marzo de 2015. Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

ISO/IEC 27044: En fase de desarrollo. Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM).

ISO 27799: Publicada el 01 de julio de 2012. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002:2005, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. Actualmente en proceso de actualización.

Este es pues el marco normativo en el cual se desenvuelve la ISO/IEC 27001:2013, al cual ha de adicionarse la ISO/IEC 29100:2011 que, aun cuando no es de la serie de la 27000, merece especial referencia como quiera que es el *framework* desarrollado por ISO/IEC específicamente para datos personales de personas naturales y que a la manera de introducción general para recién iniciados, aproxima conceptos y recomendaciones generales que han de tenerse en cuenta por las organizaciones, sin que logre un nivel mayor a simplemente constituir una introducción a las nociones del tema en tratamiento. En conclusión, todo este conjunto normativo que acompaña la ISO/IEC 27001:2013, evidencia la robustez del entorno en que la misma se desarrolla, constituyendo causa para intuirla adecuada a efectos de apalancar la búsqueda de elementos que permitan el desarrollo de un SGSDP, sumado a razones adicionales que se pasan a presentar en el numeral siguiente.

5.3 RAZONES DE ESCOGENCIA DE LA NTC/ISO/IEC 27001:2013

Tal como se ha señalado desde capítulos anteriores, el manejo de los datos personales históricamente ha sido desarrollado por las organizaciones dentro de la operación misma de la gestión de la información en general, como consecuencia lógica de constituir estos una información más de las muchas necesarias para el logro de los objetivos institucionales. En este orden de ideas, la noción de la protección de datos personales no es algo nuevo, pues de la mano del aseguramiento de la información, se venía realizando el aseguramiento de aque-

llos, obviamente sin la comprensión de su naturaleza especial y por su puesto sin las exigencias que ahora impone la ley. Es por ello que, puede decirse, la historia de tratamiento de los datos al interior de las organizaciones está íntimamente ligada con la historia del desarrollo de los instrumentos para la gestión de la información segura. De ahí que, para efectos de buscar las mejores prácticas para lograr las obligaciones de *accountability* exigidas por la LEPD, el mejor punto de partida lo constituyen, sin lugar a dudas las herramientas que para la gestión de riesgos de las organizaciones, en especial asociados a la información, se han desarrollado, toda vez que, para efectos del logro de una información segura, surgió en las organizaciones el área del gobierno de las TI, manejado a través de los sistemas de gestión de la seguridad de la información - SGSI con el propósito de, «garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías» (ISO27000.es, 2012) Esta es la razón básica por la cual se propuso el presente trabajo orientado a identificar los elementos convergentes y divergentes entre la LEPD y la NTC/ISO/IEC 27001:2013. Pero esta motivación expresada no explica por si misma el por qué esta y no otra norma o herramienta de las varias existentes. En las líneas siguientes se presentan las razones que motivaron la escogencia en particular de la norma referida.

5.3.1 ACEPTABILIDAD INTERNACIONAL

La primera de las razones de escogencia de la NTC/ISO/IEC 27001:2013, además de su objetivo que lo es orientar la implementación y la operación de los Sistemas de Gestión de Seguridad de la Información - SGSI, lo constituye el auge que ha tomado internacionalmente siendo acogida por diversas organizaciones, constituyendo ello garantía de validación en el campo real de las operaciones empresariales, que es donde se materializa el tratamiento de los datos personales. De hecho, para diciembre de 2013, contaba ya con 22.293 organizaciones en 105 países y economías, ya certificadas en la ISO/IEC27001 (Global STD, 2013).

5.3.2 CERTIFICABILIDAD DE LA NORMA

La segunda razón de la escogencia de la ISO/IEC 27001, es justamente la posibilidad de certificarse, toda vez que, al constituir norma de gestión, «define cómo ejecutar un sistema», esto es que concibe que «(…) la seguridad de la información debe ser planificada, implementada, supervisada, revisada y mejorada. Significa que la gestión tiene sus responsabilidades específicas, que se deben establecer, medir y revisar objetivos, que se deben realizar auditorías internas, etc.» (Kosutic, Diferencias y similitudes entre ISO 27001 e ISO 27002, 2010), circunstancias que en la práctica se han identificado como elementos a tener en cuenta al momento de orientar a las organizaciones al cumplimiento de la ley. En palabras de la LEPD, puede indicar de manera clara las «medidas necesarias y efectivas» para la seguridad de la información y por tanto de los datos personales claro, en perspectiva de la confidencialidad, integridad y disponibilidad. Claro está que, ha de dejarse dicho que la norma en comento se aborda en el presente trabajo, armonizada con la ISO 27002, por cuanto que, aunque,

> «Los controles de la norma ISO 27002 tienen la misma denominación que los indicados en el Anexo A de la ISO 27001; por ejemplo, en la ISO 27002 el control 6.1.6 se denomina Contacto con autoridades, mientras que en la ISO 27001 es el A.6.1.6 Contacto con autoridades» (Ibídem), el detalle cómo se abordan los controles en la ISO 27002, esto es con un nivel de mayor profundidad, aporta de mejor manera para el diseño de lo que podría ser un Sistema de Gestión de las Seguridad de los Datos Personales. En palabras de Kosutic (Kosutic, Diferencias y similitudes entre ISO 27001 e ISO 27002, 2010), se
>
> (…) podría decir que sin la descripción proporcionada por la ISO 27002, los controles definidos en el Anexo A de la ISO 27001 no se podrían implementar. Sin embargo, sin el marco de gestión de la ISO 27001, la ISO 27002 sería simplemente un esfuerzo aislado de unos pocos apasionados por la seguridad de la información, sin la aceptación de la alta dirección y, por lo tanto, sin efectos reales sobre la organización.

5.3.3 ROBUSTEZ DEL ÁMBITO NORMATIVO

La tercera razón de escogencia de la ISO 27001, como se señaló, en asocio con ISO 27002, deriva del hecho de ser parte de una gran familia de normas vinculadas con los SGSI como quedó puesto de

presente en el apartado anterior. Esta circunstancia, evidencia además la robustez y complejidad del tema de la seguridad de la información y por su puesto de los datos personales. Adicionalmente, pone de presente la enorme dificultad que le asiste a la SIC para evaluar y a las organizaciones para cumplir la exigencia reglada por la LEPD en su artículo 17 literal d y 18 literal b, correspondiente a la obligación de conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta o uso no autorizado o fraudulento, ello en concordancia con la expresión de «medidas apropiadas y efectivas» a que hace mención el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015 al exigir a las organizaciones el principio de *accountability* o responsabilidad demostrada. Por ello, es que en opinión de quien presenta este trabajo, se hace imperioso un referente a partir del cual construir un marco más preciso tanto para evaluación como para cumplimiento, el que la serie ISO 27000 y en particular la NTC/ISO/IEC 27001:2013 puede constituirlo.

5.3.4 REFERENCIA INSTITUCIONAL PARA SGSI

Una cuarta razón del por qué se escogió la norma, lo constituye el hecho de que diversos organismos de la administración pública se apalancan en la ISO 27001 para los temas de seguridad de la información. Sirven como ejemplo que el Ministerio de las TIC de Colombia, recomendara la utilización de los controles de la ISO 27002, tanto en «Entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de TI en el marco de la Estrategia de Gobierno en Línea» (Ministerio de las TIC, Colombia, 2015) y que adicionalmente se apoyara en las definiciones de la NTC/ISO/IEC 27001 para estructurar el Glosario del Manual para la implementación de la Estrategia Gobierno en línea de la República de Colombia (Ministerio de las TIC de Colombia, 2011). De igual manera lo pone de presente el que el Ministerio de Relaciones Exteriores al momento de elaborar pliegos para la actualización e implementación del modelo de seguridad de la información, exigiera dentro de los requisitos del proponente en el numeral 2.6.2.1. que el proponente esté certificado en ISO 27001-2005 (Ministerio de Relaciones Exteriores, 2011).

5.3.5 REFERENCIA NORMATIVA PARA SGSI

Una quinta razón para la escogencia de la tantas veces referida ISO 27001, lo constituyen las referencias directas que a dicha norma se realiza en el ámbito jurídico colombiano propiamente dicho. Ilustran a vía de ejemplo, entre otros casos los siguientes: La Superintendencia Financiera en su Circular Externa 052 de 2007, al incorporar el capítulo décimo segundo: requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios, en el numeral 3 sobre obligaciones generales, advierte que las entidades tienen que cumplir, como mínimo, con requerimientos tales como «3.1.2. Gestionar la seguridad de la información, para lo cual podrán tener como referencia los estándares ISO 17799 y 27001, o el último estándar disponible.» (Superintendencia Financiera de Colombia, 2007, pág. 98). Por otra parte, el Instituto Colombiano de Desarrollo Rural –Incoder–, a través de la Resolución 0314 del 5 de marzo de 2013, crea el Comité de Seguridad de la Información –CSI– del Instituto Colombiano de Desarrollo Rural –Incoder–, y al señalarle, en su artículo 4.º, numeral 5.º, dentro de sus funciones la de «Controlar el desarrollo, la implementación y el cumplimiento del Sistema de Gestión de Seguridad de la Información –SGSI–», se entiende que ha de tener en cuenta el considerando séptimo de dicha resolución que reconoce a la norma ISO 27001 como aquella que

> indica cómo puede una organización implantar un Sistema de Gestión de Seguridad de la Información, establece las directrices para la gestión del riesgo en la seguridad de la información y está diseñada para contribuir a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos (INCODER, 2013).

5.3.6 OBLIGATORIEDAD NORMATIVA

La sexta razón por la cual se ha adoptado la norma, lo es el hecho de haber sido incorporada con carácter obligatorio en ciertas disposiciones jurídicas colombianas. Son ejemplo de lo afirmado el Decreto 1465 del 10 de mayo de 2005, que reglamenta aspectos relacionados con la Planilla Integrada de Liquidación de Aportes –PILA–, que además consagró en el artículo 2, numeral 2.4, respecto del Operador de Información, la obligación contenida en el numeral 2.4.9 que a su

tenor señala: «Cumplir con el estándar de seguridad ISO 17799 –antecedente de la ISO 27001–, de manera que sus políticas y prácticas de seguridad se enmarquen dentro de dicha norma que garantiza la seguridad necesaria en el proceso de remisión y recepción de la información». Adicionalmente, el Decreto 1931 de junio 12 de 2006, que modificó parcialmente el anterior, nuevamente, en el artículo 3, sobre condiciones de operación del sistema PILA, en el numeral 3.4, párrafo 5, advierte que «Para garantizar la idoneidad del servicio al que se refiere el presente numeral, los Operadores de Información deberán certificar el cumplimiento de la norma ISO 27001, a más tardar en un año a partir de la entrada en vigencia del presente decreto.» (Se subraya fuera de texto).

5.3.7 CONDICIÓN DE NORMA TÉCNICA COLOMBIANA –NTC–

Finalmente, como séptima y última razón de escogencia de la ISO 27001, lo constituye la decisión del Icontec de adoptarla como norma técnica colombiana, bajo la denominación de NTC/ISO/IEC 27001. Cabe recordar que el Icontec, quien además ostenta la condición de miembro con derecho a voz del Consejo Nacional de Normas de Calidad por mandato del Decreto 2152 de 1992, es el Organismo Nacional de Normalización, lo que significa que, conforme al artículo 2, literal f, del Decreto 2269 de 1993 modificatorio parcialmente del Decreto 2746 del 6 de noviembre de 1984, refrendado por el Decreto 1471 de 2014, artículo 8, es la «Entidad reconocida por el Gobierno Nacional cuya función principal es la elaboración, adopción y publicación de las normas técnicas nacionales y la adopción como tales de las normas elaboradas por otros entes.» Adicionalmente, el Icontec se encuentra acreditado, entre otras, como Organismo de Certificación de Sistemas de Gestión de Seguridad de la Información por el Organismo Nacional de Acreditación –ONAC– (corporación sin ánimo de lucro de naturaleza y participación mixta, regida por las normas del derecho privado (ONAC, 2010).

En desarrollo de las funciones adjudicadas y las competencias desarrolladas, el Icontec, mediante decisión del Consejo Directivo del 22 de marzo de 2006, ratificó como norma técnica colombiana la ISO/IEC 27001:2005 y posteriormente el 11 de diciembre de 2013

mediante decisión del mismo Consejo, aprobó la primera modificación mediante la cual se adoptó la ISO/IEC 27001:2013. Para realizar tal declaración, se surtió un trámite por parte de un grupo significativo de representantes de empresas que, con su acción en el comité de estudio, reconocieron como adecuado el protocolo normativo para el ámbito de las organizaciones. El grupo de entidades que participaron en el proceso de estudio y aprobación fueron: Avianca S. A., Azteca Comunicaciones, Banco Agrario de Colombia S. A., Cenet S. A., Cross Border Technology S. A. S., Ecopetrol-Slb, Esicenter-Sinertic, Geoconsult-Ecp, Halliburton-Ecopetrol, Helm Bank, Infotrack S. A., Inlac, La Polar-Cf, Ministerio de Tecnologías de la Información y las Comunicaciones, Newnet S. A., Project Advanced Management, Qualitic Ltda, Servientrega y Top Factory. Posteriormente la norma fue sometida a consulta ante un grupo de más de 100 empresas. Solo una vez cumplido el trámite antes mencionado, la norma se adoptó como NTC/ISO/IEC 27001:2013.

El hecho de haber sido reconocida la ISO/IEC 27001 como NTC ha implicado que, conforme al Decreto 1471 de 2014, artículo 7, numeral 55, sea considerada como:

> Documento aprobado por una institución reconocida, que prevé, para un uso común y repetido, reglas, directrices o características para los productos o los procesos y métodos de producción conexos y cuya observancia no es obligatoria. También puede incluir prescripciones en materia de terminología, símbolos, embalaje, marcado o etiquetado aplicables a un producto, proceso o método de producción o tratar exclusivamente de ellas (subrayado fuera de texto).

Esta definición es copia textual de la contenida en el Anexo 1 del Acuerdo sobre Obstáculos Técnicos al Comercio y que hace parte de los acuerdos de la Organización Mundial del Comercio –OMC–. Por tanto, su contenido normativo, al ser de obligatorio acatamiento para Colombia por ser miembro desde el 30 de abril de 1995 (Organización Mundial de Comercio –OMC–, 2014, pág. 62) implica que la NTC/ISO/IEC 27001:2013 no sea obligatoria, salvo, como quedó señalado, cuando una norma jurídica colombiana así lo establezca para un propósito específico.

Por todo lo expuesto, la NTC/ISO/IEC 27001:2013 constituye un buen referente normativo no obligatorio, para, apoyar en ella la búsqueda de elementos orientadores para la gestión de *accountability*,

partiendo de la definición de los elementos convergentes y divergentes de esta con la LEPD.

5.4 PRINCIPIOS RECTORES DE LA NTC/ISO/IEC 27001

La norma NTC/ISO/IEC 27001, tal como se observa en el Anexo B de aquella y cuya naturaleza no es normativa sino informativa, lo cual significa que no es materia del componente certificable, posee un conjunto de principios rectores basados en 7 de los 9 principios que la OCDE ha consagrado en las Directrices para la Seguridad de Sistemas y Redes de Información (OCDE, 2002). Los principios adoptados son los siguientes:

5.4.1 PRINCIPIO DE CONCIENCIACIÓN

«Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.»

5.4.2 PRINCIPIO DE RESPONSABILIDAD

«Todos los participantes son responsables de la seguridad de los sistemas y redes de información.»

5.4.3 PRINCIPIO DE RESPUESTA

«Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad».

5.4.4 PRINCIPIO DE VALORACIÓN DE RIESGOS

«Los participantes deben llevar a cabo evaluaciones de riesgo».

5.4.5 PRINCIPIO DE DISEÑO E IMPLEMENTACIÓN DE LA SEGURIDAD

«Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.»

5.4.6 PRINCIPIO DE GESTIÓN DE SEGURIDAD

«Los participantes deben adoptar una visión integral de la administración de la seguridad.»

5.4.7 PRINCIPIO DE REEVALUACIÓN

Los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

Como nota significativa se reseña que la ISO/IEC 27001 no incorporó, y por tanto la NTC correspondiente tampoco, los principios OCDE de Ética (4.º), según el cual «Los participantes deben respetar los intereses legítimos de terceros», fundamentado en el reconocimiento del riesgo a terceros por la utilización de la información en especial la «y la protección apropiada de información personal», ni de Democracia (5.º), según el cual «La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática» dentro de los cuales refiere, entre otros la «confidencialidad de la información» (OCDE, 2002, págs. 8, 9). Esta omisión contrasta con el hecho de observar como en el anexo A de la NTC/ISO/IEC 27001 (de naturaleza normativa), en la Tabla A.1. correspondiente a los objetivos de controles y controles, en el apartado A.18 Cumplimiento, en el control A.18.1.4, se tiene planteado el control «Privacidad y protección de información de datos personales», describiéndose para la búsqueda del cumplimiento de las legislaciones sobre la materia. La explicación que pudiere darse a dicha omisión, desde la óptica de quien presenta este trabajo, es quizá la naturaleza del objeto materia de protección de la norma NTC/ISO/IEC 27001 y la lógica de sus gestores, esto es, considerar la norma

dirigida, eminentemente destinada a la seguridad de un activo sin relación alguna con los terceros involucrados con él, donde los aspectos humanos de la información no son tenidos en cuenta al momento de diseñarse un SGSDI. En otras palabras, la seguridad de la información, como se ha dicho a lo largo del trabajo, ha buscado proteger el patrimonio de las organizaciones con un criterio exclusivamente económico.

Independientemente de la omisión puesta de presente en el párrafo anterior, resulta de interés sí relievar la participación que la ISO/IEC le reconoció a la OCDE al momento de definir los principios de la 27001. Esta circunstancia convierte a la OCDE en un punto común entre la norma 27001 y la LEPD.

5.5 ELEMENTOS INTEGRADORES DE LA NTC/ISO/IEC 27001

Referenciado como se han efectuado las condiciones históricas de surgimiento de la norma ISO/IEC 27001, su objetivo constituido por la implementación de los Sistemas de Gestión de la Seguridad de la Información - SGSI, al ámbito normativo en el que se desarrolla y al que pertenece (serie 27000), las razones de la escogencia de la misma para los propósitos del presente trabajo y los principios que le orientan, corresponde ahora identificar algunos de los elementos que se consideran constitutivos de dicha norma, entre otras con el propósito posterior correlación con la LEPD.

5.5.1 NÚCLEO ESENCIAL DE PROTECCIÓN DE LA NORMA NTC/ISO/IEC 27001

Constituye el núcleo de una norma estándar el objetivo perseguido por ella. En tratándose de la NTC/ISO/IEC 27001, del cuerpo de la norma se identifica el mismo en los siguientes términos:

> (…) implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La presente Norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización (ICONTEC, 2013, pág. 1).

Tres aspectos constituyen entonces, conforme a la transcripción efectuada, el núcleo de la norma en referencia a saber: a) La implementación de un SGSI, b) el mantenimiento del mismo y c) la mejora continua.

Para efectos de la implantación del SGS la norma 27001 se apalanca en la Guía Técnica Colombiana GTC/ISO/IEC 27003:2012 (Icontec, 2013), que contiene las recomendaciones a seguir para la implementación de un SGSI. Esta norma, no obstante haber sido aprobada en el año 2012, aún mantiene el modelo PHVA (planear, hacer, verificar y actuar) que en el cambio de la norma 27001 del año 2005 a la versión 2013 se suprimió en su referencia.

El proceso de implementación estará determinado por el alcance que se le desee dar al SGSI, es decir que al interior de una organización puede aplicarse por ejemplo a un servicio o producto de los varios que formen parte del *core* de la organización, a una división o una parte de ella, en fin, puede ser sectorizada su implementación.

5.5.2 LA INFORMACIÓN COMO OBJETO DE PROTECCIÓN DE LA NTC/ISO/IEC 27001

Definido el objetivo de la norma como la implantación y gestión de un SGSI, debe señalarse que el objeto de la misma lo constituye la información propiamente dicha. Para comprender tal concepto, cabe en primer lugar acoger la acepción 5.ª que de información provee la Real Academia de la Lengua Española, esto es «Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada» (Real Academia Española, 2014). Ahora bien, sin el propósito de ahondar en disquisiciones que corresponden al campo de la epistemología y por considerar un tanto limitada la definición de información antes referida, para los fines de este trabajo y en función de las operaciones de las organizaciones, ámbito donde entre otras se materializa el relacionamiento con ella y de contera con los datos personales, cabe ampliarla en términos de Rafael Capurro, para entender la información como conocimiento aplicado a una demanda concreta, donde la información no corresponde simplemente al «matching de un dato de entrada (input) con otro dato previamente fijado, sino que dicho dato fijado es concebido como una oferta frente a la cual el usuario juega un rol eminentemen-

te activo» (Capurro, 2007, pág. 22). Es decir que la información se entiende como conocimiento aplicado, fruto del relacionamiento intersubjetivo del observador/operador con la realidad, expresado a través de códigos lingüísticos y puesta al servicio de un usuario que interactúa con ella (para quien desee ahondar en las nuevas dimensiones epistemológicas del conocimiento y la información, se recomienda consultar acerca de la cybersemiótica). En tal sentido, podemos decir que constituye información, por ejemplo, el proceso de organización de las operaciones de una empresa, el cómo se desarrolla la producción de bienes o servicios que ella provee, también las redes de relacionamiento con proveedores y por su puesto con consumidores o clientes externos, adicionalmente es información el conjunto de los insumos necesarios para la operación misma y por sobre todo el talento humano que la ejecuta, al igual que la identificación de cada uno de los interesados (socios, comunidad relacionada, etc.) así como las demandas que esperan ser satisfechas, entre otros muchos aspectos. Justamente, al entender la información desde esta dimensión que permite ver la diversidad de elementos que la constituyen y por tanto la complejidad para su adecuada gestión, aumentada de manera directamente proporcional al tamaño de la organización correspondiente, se explica la necesidad de generar un sistema que asegure contar con ella en el momento en que se requiera, con la certeza de saberla cierta y completa, debidamente asegurada para evitar la accesibilidad de terceros no autorizados y, si dentro de dicha información se encuentran datos personales, acorde con las exigencias legales pertinentes.

5.5.3 CLASIFICACIÓN DE LA INFORMACIÓN

La norma 27001 en análisis no provee una clasificación de la información, ni establece unos criterios directos para efectuar tal ejercicio. Sin embargo, en la tabla A.1 del anexo A, dominio A.8 Gestión de Activos, Subdominio A.8.2 Clasificación de la Información, en el control A.8.2.1. define los criterios que deben tenerse en cuenta para clasificar la información así: a. Según los requisitos legales, b. Valor de la información para la organización, c. Criticidad de la información, d. Susceptibilidad de la divulgación, e. Susceptibilidad a modificaciones no autorizadas (ICONTEC, 2013, pág. 15)

Estas líneas generales de clasificación debieran interpretarse de la mano del desarrollo que de ellas hace la ISO 27002, Control 8 Gestión de Activos, Control 8.2 Clasificación de la Información, sin embargo, esta norma de soporte no contribuye de manera significativa, limitándose a adicionar, a lo ya afirmado por la 27001 que «Se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento» (iso27000.es, 2005).

Teniendo en cuenta que el objetivo del presente acápite es el de describir la NTC/ISO/IEC 27001:2013, no pudiera pasarse por alto, frente a la falencia advertida, que en Colombia la información, en perspectiva de la seguridad de la misma (se advierte, no de la seguridad de los datos personales) se encuentra reglada en la Ley 1712 de 2014 por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, aplicable a todas las entidades públicas y particulares señaladas en el artículo 5.º Con base en dicha norma, la Presidencia de la República expidió la Guía Para la Calificación de La Información de acuerdo con sus Niveles de Seguridad (Presidencia de la República de Colombia, 2015), que, en tratándose de entidades oficiales puede servir de orientación a los interesados en profundizar este aspecto. En cuanto hace referencia a entidades privadas no obligadas por la Ley 1712 de 2014 habrá de tenerse presente los criterios arriba expuestos por la ISO 27002.

5.5.4 PROPIETARIO Y RESPONSABLE DE LA INFORMACIÓN

El concepto que la norma NTC/ISO/IEC 27001:2013 posee de propietario de la información no puede entenderse en la dimensión jurídica del derecho de propiedad. Acá, la propiedad hace referencia a la condición de relación que se establece entre un funcionario de la organización y un activo (para el caso la información física o digital) que, en razón de los roles y competencias que le han sido asignadas, le genera el deber de responder por él. Este es el sentido del control A.8.1.2 Propiedad de los activos, del Subdominio A.8.1. Responsabilidad de los Activos, del Dominio A.8 de la Tabla A.1. del anexo A de dicha norma, cuando advierte que «los activos mantenidos en un inventario deben tener un propietario» (ICONTEC, 2013, pág. 15).

En todo caso, no debe confundirse el concepto de propietario de la información con los responsables de la información, pues corresponden a dos roles diferentes. En el primer caso, se hace referencia a aquellas personas que, en virtud de la labor que les corresponde realizar (contador, revisor fiscal, auditor, vigilante, etc.), requieren del manejo de cierta información, motivo por el cual forma parte de las obligaciones propias de su cargo el velar por aquella. Los segundos, esto es los responsables de la información hacen referencia a actores propiamente dichos de un SGSI que dependiendo del tamaño de la organización deberán ser más o menos los actores correspondientes. Gustavo Pallas (Pallas Mega, 2009, pág. 28) por ejemplo, refiere que organizaciones medianas y grandes:

> (…) se presenta la necesidad de tener un responsable de seguridad para cada orden o contexto jerárquico de la empresa, es decir: un responsable global de la seguridad de IT, un responsable de la seguridad de IT por Área, y un responsable de la seguridad por proyecto/ sistema. Adicionalmente se presenta la necesidad de un comité responsable de la coordinación de la seguridad de IT, y un equipo responsable de gerenciar la seguridad de IT. Este último coordina actividades globales a la organización, da lineamientos globales y gerencia las diferentes fases del sistema de gestión de seguridad, dando soporte a los oficiales de seguridad de los diferentes contextos (global, área, proyecto/ sistema).

5.5.5 OTROS ELEMENTOS INTEGRADORES

Adicionalmente han de tenerse como elementos integradores de la Norma NTC/ISO/IEC 27001:2013 los siguientes:

- La Infraestructura TIC: software, hardware y redes, con el que se opera la gestión de la información.
- Protocolos de Seguridad: El conjunto de normas que recogen las buenas prácticas en materia de gestión de la seguridad de la información.
- Organismo Nacional de Acreditación: organismo encargado de reconocer a otro la capacidad de certificar el cumplimiento. Para el caso colombiano Organismo Nacional de Acreditación –ONAC.
- Autoridad de Normalización: organismo encargado de aprobar la norma que contiene el estándar, para el caso de Colombia ICONTEC.

- Organismo de Certificación de Sistemas de Gestión de Seguridad de la Información: organismos encargados de certificar el cumplimiento del estándar. Para el caso colombiano Icontec, entre otras. Se incorporó al texto original.

6. ELEMENTOS CONVERGENTES Y DIVERGENTES ENTRE LA LEPD Y LA NTC/ISO/IEC 27001

Cumplidas las fases previas, basadas en un ejercicio analítico descriptivo del Hábeas Data en Colombia (LEPD) en perspectiva de la dignidad y de la norma internacional de gestión de seguridad de la información NTC/ISO/IEC 27001:2013, que permitió la visualización desde los orígenes, marcos normativos, objetivos y objetos, actores y desarrollos normativos, entre otros elementos, corresponde ahora poner de presentes los resultados obtenidos del ejercicio analítico reflexivo que buscó identificar los elementos convergentes y divergentes entre las normas en mención así:

6.1 **ELEMENTOS CONVERGENTES**

Sin lugar a dudas pueden ser muchos más los elementos convergentes existentes entre la NTC/ISO/IEC 27014:2013 y la LEPD, sin embargo, los que a continuación se presentan, corresponden a aquellos que, en criterio de quien desarrolla el presente trabajo, son los de mayor relevancia para ulteriores propósitos.

6.1.1 ÁMBITO DE ACCIÓN U OPERATIVIDAD

Uno de los elementos convergentes entre la LEPD y la NTC/ISO/IEC 27001, es justamente el ámbito de acción u operatividad de los objetos de cada una de las normas. Esta afirmación se basa en que la información en general y por tanto los datos personales, entendidos como una manifestación específica de aquella, son objeto de operaciones en el marco de los procesos desarrollados por las organizaciones (estratégicos, misionales, de apoyo, transversales, etc.). Así incluso lo reconoció la Corte Constitucional en sentencia T-729 de 2002 ya referida, en relación con el Hábeas Data, aplicable en general a la información, al afirmar que:

> El ámbito de acción o de operatividad del derecho al Hábeas Data o derecho a la autodeterminación informática, está dado por el entorno en

el cual se desarrollan los procesos de administración de bases de datos personales. De tal forma que integran el contexto material: el objeto o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos.

6.1.2 GESTIÓN SISTÉMICA DE LA SEGURIDAD

Del ejercicio analítico descriptivo efectuado de la NTC/ISO/IEC 27001 y de la LEPD se pudo identificar claramente que es común el propósito que dichas normas buscan, esto es, la gestión sistémica y segura de la información y de los datos personales. La primera a través de los SGSI y los segundos a través de las medidas apropiadas y efectivas (artículo 2.2.2.25.6.1 del Decreto 1074 de 2015).

Concatenado el primer elemento convergente del Ámbito de Acción con este segundo, puede entonces decirse que el propósito normativo de ambas disposiciones, está directamente implicado en el área de gestión de los riesgos de las organizaciones, pudiéndose expresar de manera más evidente, apoyados en el diagrama de *venn* inicialmente elaborada por Kosutic, con la siguiente figura:

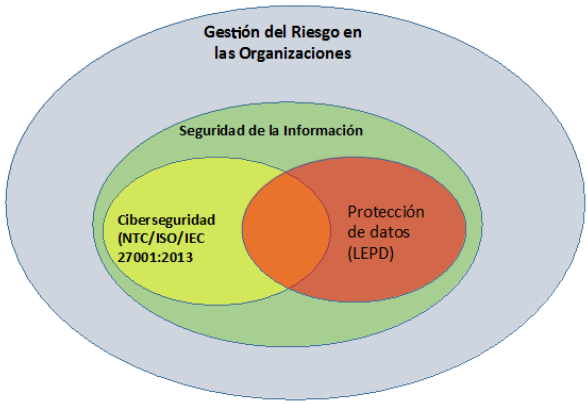


Figura 23. *Propósito normativo de la LEPD y la NTC/ISO/IEC 27001:2013*

«En el universo de la gestión de los riesgos de las organizaciones, han de articularse, como coadyuvantes del área de seguridad de la información, los aportes de la norma ISO 27001 y los de las de la normativa de protección de datos personales.»

La figura muestra ese espacio común que comparten las dos disposiciones y que se refuerza con la circunstancia de la exigencia del Principio de valoración de Riesgos de la norma ISO, según la cual, como quedó dicho, manda que «Los participantes deben llevar a cabo evaluaciones de riesgo», muy en la línea de la exigencia del artículo 2.2.2.25.6.1 del Decreto 1074 de 2015, mencionado inmediatamente atrás, según el cual la dimensión de los mecanismos apropiados y efectivos deberán desarrollarse con base, entre otras, a los riesgos potenciales que el tratamiento de los datos pudiera causar a los titulares de los mismos. Esta característica de necesidad de gestión sistémica de la seguridad y, por su puesto, de los datos personales, lo ha puesto de manifiesto el INAI en México cuando, a finales del año anterior dio a conocer la segunda versión de la Guía para implementación de un Sistema de Gestión de Seguridad de Datos Personales (INAI, 2014), respecto de la cual, cabe destacar el gran valor que aporta al propósito de orientar el adecuado tratamiento de datos personales, sin perjuicios de algunos aspectos que se consideran debieran ser objeto de discusión como la falta de ciertos los nuevos controles incorporados por la ISO 27001:2013, la propuesta de la formulación de la PTI en la fase 2 de la planeación cuando ella debe ser fruto casi final de la intervención como incluso lo orienta la GTC/ISO/IEC 27003, ello como consecuencia entre otras del exagerado apego que aún se evidencia a la versión 2005 de la ISO 27001 que incluía como marco metodológico el modelo «Planificar-Hacer-Verificar-Actuar» (PHVA) que, en la versión 2013 ya no se incluye su referencia.

6.1.3 EXPOSICIÓN DE LOS OBJETOS PROTEGIDOS A RIESGOS COMUNES

Asociado al propósito normativo, otro elemento convergente entre las dos normas materia de análisis lo es el hecho de la identidad entre algunos de los riesgos a que están sometidos los objetos de protección de cada una de ellas. Si bien es cierto existen riesgos propios de cada una de las áreas normativas y sobre los cuales se hará alguna referencia renglones adelante en los aspectos divergentes, resulta de interés precisar que los riesgos asociados al acceso no autorizado de terceros a la información y a los datos pueden ser comunes. Son, por ejemplo, los ataques activos y pasivos a los sistemas lógicos que con-

tienen la información en general y/o los datos personales en particular, según William Stalling (Stalling, 2004), se describen así:

> Ataques pasivos: Los ataques pasivos se dan en forma de escucha o de observación no autorizadas de las transmisiones. El objetivo del oponente es obtener información que se esté transmitiendo. Dos tipos de ataques pasivos son la obtención de contenidos de mensajes y el análisis de tráfico (sniffing) (…) Un segundo tipo de ataque pasivo, el análisis de tráfico, es más sutil. Supongamos que hemos enmascarado los contenidos de los mensajes u otro tráfico de información de forma que el oponente, incluso habiendo capturado el mensaje, no pueda extraer la información que contiene. (…) La técnica común para enmascarar los contenidos es el cifrado. Incluso si tuviésemos protección mediante cifrado, un oponente podría observar el patrón de los mensajes, determinar la localización y la identidad de los servidores que se comunican y descubrir la frecuencia y la longitud de los mensajes que se están intercambiando. Esta información puede ser útil para averiguar la naturaleza de la comunicación que está teniendo lugar. Los ataques pasivos son muy difíciles de detectar ya que no implican alteraciones en los datos.
>
> Ataques activos: Los ataques activos implican alguna modificación del flujo de datos o la creación de un flujo falso y se pueden dividir en cuatro categorías: suplantación de identidad, repetición, modificación de mensajes e interrupción del servicio.
>
> Una **suplantación** se produce cuando una entidad finge ser otra. (…). La **repetición** implica la captura pasiva de una unidad de datos y su retransmisión posterior para producir un efecto no autorizado. La **modificación** de mensajes significa que una parte de un mensaje original es alterada, o que los mensajes se han retrasado o reordenado, para producir un efecto no autorizado. (…) La **interrupción del servicio** impide el uso o la gestión normal de las utilidades de comunicación (Stallings, 2004, págs. 8-9).

6.1.4 FUNDAMENTACIÓN EN PRINCIPIOS

No obstante, algunos aspectos diferenciadores en materia de principios aplicables a cada una de las normas y que serán puestos de presente en aparte posterior, si constituye un aspecto convergente entre las disposiciones en análisis, la circunstancia de que su reglamentación se inspira en principios. Dentro de ellos incluso pueden apreciarse algunos comunes como por ejemplo el denominado Principio de Seguridad del Hábeas Data ordenado por la Ley 1581 de 2012, artículo 4, literal g, y el 8.º principio de las Directrices para la Seguri-

dad de Sistemas y Redes de Información (OCDE, 2002) esto es el Principio de Gestión de Seguridad.

6.1.5 REQUERIMIENTO DE POLÍTICA

Tanto la ISO como la LEPD, coinciden en la necesidad de definir una política para la organización, de tal manera que oriente de forma general pero clara, y de acuerdo a las operaciones propias de cada entidad, la gestión de la información y de los datos, respectivamente, obvio con exigencias diferenciadas para cada uno de ellas. Debe insistirse que, conforme a la metodología de implantación de la ISO, la definición de la política es una tarea incluso efectuada antes de la realización de los análisis de amenazas, vulnerabilidades y riesgos, no obstante que la ISO 27003 indica que al final debe revisarse nuevamente. Mientras que, aun cuando la LEPD no señala un proceso de implantación en las organizaciones y por lo tanto no dice si la elaboración de la política debe ser al inicio o al final del proceso de implantación inicial, por la experiencia y discrepando de lo dispuesto por la Guía del INAI, la PTI debe ser elaborada al final del proceso de implantación inicial, pues solo después de identificar los componentes esenciales del sistema de gestión de seguridad de datos personales –SGSDP (procesos que involucran datos, titulares y datos caracterizados, infraestructura TIC y locaciones físicas de bases de datos no digitales involucradas), descritas las líneas bases conforme a los presupuestos de conformidad que se definan para el análisis de riesgos, desarrollada la tarea de identificación de amenazas, vulnerabilidades y riesgos, en fin, solo una vez conocida al máximo la realidad de la operación de los datos personales, puede realizarse la Política de Protección de la Información –PTI–, para ahí sí aprobarla por el órgano competente de la dirección. Si se acogiera la propuesta de la ISO o del INAI, para el caso colombiano que exige antes de la aprobación de la dirección la notificación de la PTI a los titulares antes de la aprobación, se estaría seguramente haciendo sin sentido dos veces el trámite en un muy corto lapso, uno al inicio y otro al final de la implantación inicial, dando entre otras un mensaje de desorganización institucional a los titulares, quienes en las más de las veces son justamente clientes de las organizaciones, con riesgo de afectaciones al *good will* que se haya logrado desarrollar.

6.1.6 ACTORES RESPONSABLES

La existencia de responsables tanto de la información como de los datos, constituye una exigencia común en las dos normas existentes.

En tratándose de la ISO se han llegado a establecer diferentes roles en función de la responsabilidad de la información. Dentro de ellos se pueden destacar: los DBA *(database administrator)* o Administradores de Bases de Datos, a quienes compete, entre otras responsabilidades, el aseguramiento de las bases de datos automatizadas, la implementación y gestión de copias de respaldo o *backups* y, en el evento de desastres que impliquen afectación de la información residenciada en ellas, adelantar las labores de recuperación que fuere menester. Otro responsable de la información es el Oficial de Seguridad de la Información o Director de Seguridad de la Información, también llamados CISO por sus siglas en inglés *(chief information security officer)*. A este actor de la información se le encomienda, entre otras la responsabilidad de asegurarse el cumplimiento regulatorio conforme a los elementos normativos (interno y externo) exigidos en cada caso para la seguridad de la información. Adicionalmente a los anteriores, también se identifica como responsable de la información al Oficial de Arquitectura de la Información, a quien se le encomienda, entre otras el diseño y gestión de los procesos de seguridad del negocio, estructura organizacional, seguimiento de inventarios de seguridad técnicos. Estos roles y otros más son desagregados o concentrados en una sola persona o área según la robustez de la organización y la operación TI que la misma desarrolle.

Por su parte la LEPD además de asignar las categorías de Responsable y Encargado a la organización que trata datos personales (artículo 17 y 18 de la LEPD), en lo que hace referencia a personal o área responsable de los datos, sólo se limita a exigir la designación de uno u otra para que asuma «la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012» (artículo 2.2.2.25.4.4 del Decreto 1074 de 2015). En el ámbito europeo se ha establecido con carácter obligatorio la figura del Responsable de Protección de Datos Personales al interior de las organizaciones (Consejo de la Unión Europea, 2015).

En la práctica se ha identificado que, no resulta suficiente la dimensión obligacional tal como lo expresó el decreto reglamentario de la LEPD, pues en organizaciones medianas o grandes se requiere una estructura un poco más compleja para efectos de ejercer el gobierno de lo que se ha denominado sistema de gestión de seguridad de datos personales –SGSDP–. En esos casos se recomienda la creación de un comité de protección de datos personales, con responsables de los ámbitos de procesos, TIC, bases documentales, locaciones físicas y atención de PQR, entre otras asignaciones funcionales relacionadas con el tratamiento de los datos.

6.1.7 GESTIÓN DE INCIDENTES

Otro elemento convergente entre las dos normas, y es lógico de entender, es la necesidad de reaccionar a los eventos en que se producen incidentes de seguridad, entendido como «Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información» (Salcedo B., 2014) o de los datos personales, se agrega.

Para tal propósito la NTC/ISO/IEC 27001, en el Anexo A, en la Tabla A.1 (normativo) en el Dominio A.16, establece la gestión de incidentes de seguridad de la información, con un conjunto de controles dentro de los cuales puede destacarse el A.16.1.2 que corresponde a los Reportes de eventos de seguridad de la información, ordenando reportarlos a través de canales de gestión apropiados, tan pronto como sea posible. Esta disposición de la ISO 27001 se complementa con la guía técnica colombiana GTC/ISO/IEC 27035, la que habiendo sido ratificada por el Consejo Directivo de Icontec el 12 de diciembre de 2012, está dedicada especialmente a la gestión de los incidentes de seguridad de la información.

Por su parte la LEPD en el artículo 18 establece como obligación de los Encargados, y ha de entenderse también de los Responsables así el artículo 17 de la misma norma no lo diga, el reportar a la «Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares».

6.1.8 DOCUMENTACIÓN COMÚN

De la descripción normativa efectuada, articulada con la experiencia en campo, se ha identificado como elemento convergente, la exigibilidad en materia de levantamiento de documentación para efectos de las evidencias del cumplimiento de la ISO o de *accountability*, en el caso de la LEPD.

De hecho, la NTC/ISO/IEC 27001, en el área denominada Seguridad de las Operaciones, y de manera puntual, entre otros, en el control A.12.1 correspondiente a Procedimientos de operación documentados, ordena que «los procedimientos de operaciones se deben documentar y poner a disposición de todos los usuarios que los necesitan» (ICONTEC, 2013). Adicionalmente obliga a gestionar documentadamente los cambios que se den en la organización, en procesos, en instalaciones y en los sistemas como lo ordena el control A.12.2 (ICONTEC, 2013).

En el caso de la LEPD, aun cuando hay diversas referencias al deber de documentar (conservación de las autorizaciones, registro de incidentes, etc.), hoy en día, con ocasión de la expedición de la Guía de la Implementación del Principio de Responsabilidad Demostrada por parte de la Superintendencia de Industria y Comercio de Colombia (Superintendencia de Industria y Comercio, 2015) y las exigencias incorporadas en el Registro Nacional de Bases de Datos (Superintendencia de Industria y Comercio, 2015), se han identificado una serie de controles que generan la necesidad de llevar la documentación de ciertos registros.

Dentro de los registros que, normalmente utilizados en los SGSI que se detectaron como útiles para efectos de *accountability* y RNBD en relación con el Hábeas Data, se identificaron los siguientes:

1. Registro de control de dispositivos removibles o soportes móviles de almacenamiento: Se busca que la organización que utiliza este tipo de dispositivos con datos personales, esté referenciado a un usuario específico, para poder saber, en eventos de incidentes, quien responde.

2. Registro de seguimiento de eliminación de dispositivos removibles de almacenamiento. Se busca hacer seguimiento al proceso de eliminación de este tipo de dispositivos cuando se han alojado datos personales en ellos.

3. Registro de entrada y salida de medios de almacenamiento. Se busca hacer seguimiento a la movilidad de datos personales fuera de la organización, cuando ello es imperativo.

4. Registro de actividades de los usuarios. Se busca darle trazabilidad a la actividad de los usuarios en los sistemas y en las redes con que se tratan datos personales.

5. Registro de usuarios nuevos, altas, bajas y modificación en forma o privilegio. Se busca tener la identificación de todos y cada uno de los miembros del talento humano a quienes se les autoriza acceso a los sistemas que tratan datos personales.

6. Formato de solicitud de creación y cancelación de cuentas de usuario y Registro de monitoreo de actividades. Se busca tener un registro de las solicitudes que se hacen de usuarios de los sistemas que tratan datos personales.

7. Registro de asignación de privilegios. Se busca dejar constancia de los privilegios que, conforme a los roles, se les adjudica a cada uno de los usuarios en los sistemas, redes, directorios activos, etc.

8. Registro de verificación de roles y privilegios. Se busca dar trazabilidad a los cambios de privilegios para evitar escalamiento a privilegios no autorizados facilitando el acceso a datos personales.

9. Registro de modificación o retiro de derechos de acceso y cambio de dependencia. Se busca dar constancias de modificaciones cuando hay cambio de dependencia, a fin de evitar acceso, o asegurarlo según se requiera, a datos personales.

10. Registro de control de acceso. Se busca establecer o corroborar los mecanismos de registro de control de acceso físico y de acceso a las redes y sistemas de información de la organización, para auditar el acceso a la información por parte de personal con cargos o roles que no tienen contacto con la información o que no la utilizan. Para efectos prácticos llevar un registro de ingreso/salida a las áreas restringidas y al archivo, y un registro de inicio y cierre de sesión en los sistemas de información que contienen datos personales. El propósito es de auditoría y genera trazabilidad.

11. Registro de control de contraseñas. Es un registro diseñado específicamente para controlar los cambios de contraseña en los usuarios de sistemas de información, que identifica de manera especí-

fica el área donde se realiza el cambio de contraseña. Genera trazabilidad y tiene propósitos de auditoría.

12. Registro de control de actividades realizadas con cuentas críticas. Permite hacer trazabilidad a los cambios necesarios específicamente en una cuenta de usuario que tenga roles o privilegios superiores altamente restringidos, es decir, cuentas de administración o supervisión que por tanto tendrían acceso a datos personales. Genera evidencia en los motivos por los cuales fue necesario interactuar con dichas cuentas y los cambios realizados.

13. Registro de asignación de llaves criptográficas. Permite la administración y control sobre las llaves de cifrado en los sistemas criptográficos de una organización, identifica el sistema de gestión de llaves, los sistemas de información donde se implementa cada llave de cifrado y las características técnicas de cada una. Es un registro crítico porque contiene datos que permiten el acceso a datos sensibles.

14. Registro de control de acceso físico. Registro que permite registrar la información del personal que accede a las áreas restringida en una organización, se puede implementar en áreas restringidas y áreas de acceso generales e incluye el control de ingreso a dispositivos que contengan datos personales. Es un registro de propósito general que se debe incluir en auditorías.

15. Registro de mantenimientos de equipos. Registro que permite trazabilidad en la gestión de los mantenimientos realizados a los equipos que procesan o almacenan información digital que contenga datos personales. Registro de propósito general que aporta información en auditorías.

16. Registro de reutilización y retiro de equipos. Registro del tipo de borrado y/o método de destrucción que permite control, trazabilidad y cumple propósitos de auditoría en los equipos que han tratado datos personales y que se reutilizan en áreas diferentes a su origen o que se retiran de la operación.

17. Registro de control de copias de seguridad. Registro crítico para una organización, pues indica los parámetros técnicos generales en el proceso de generación de copias de seguridad de las bases de datos que contienen datos personales. Tiene propósitos de trazabilidad y auditoría. De suma importancia cuando las copias se encuen-

tran en servicios de alojamiento en países diferentes a Colombia, puede implicar transferencia internacional.

18. Registro de vulnerabilidades técnicas. Busca llevar un registro de las vulnerabilidades encontradas y el nivel del riesgo según la criticidad de los datos personales.

19. Registro de accesos remotos. Permite llevar control de los usuarios que requieran accesos remotos para el desarrollo de sus actividades y los elementos de red de los cuales hace uso.

20. Registro de control de cambios de sistemas. Permite controlar los cambios de los sistemas de informáticos que se utilizan en el tratamiento de datos personales, basándose en los requerimientos realizados por las diferentes áreas o dependencias de la organización.

21. Registros de reporte de incidentes de seguridad e historial de incidentes de seguridad de la información. El registro de reporte permite llevar un control de los incidentes de seguridad que afectan la disponibilidad, confidencialidad e integridad de la información que contiene datos personales y contiene la información detallada del incidente y los elementos de hardware, software e información que se vieron afectados. Sus resultados deben ser reportados al Registro Nacional de Bases de Datos que ejecuta la SIC a través de la plataforma web que para el efecto se ha habilitado.

22. Registro de privilegios de acceso a bases de datos. Permite llevar un control de los sistemas lógicos que alojan bases de datos en cuanto a que información tienen derechos de acceso los usuarios de la red corporativa, según sus roles y responsabilidades.

23. Registro de aprobación de políticas y protocolos del SGSDP y de cambios de los mismos. Se busca llevar el registro y control de las normas internas que, así como regulan los SGSI, pueden estar regulando el SGSDP. Esto además por cuanto que, en tratándose de la LEPD, cuando se dan cambios estructurales en los componentes del sistema (cambio de titulares, captura de nuevas tipologías de datos, modificación o incorporación de nuevas finalidades, cambio de los canales de atención, etc.) deben efectuarse modificaciones entre otras de la misma PTI.

6.1.9 AUTORIDADES NORMATIVAS

Otro elemento convergente lo constituye la existencia en relación con cada una de las normas cotejadas, de «autoridades» que verifican el proceso de cumplimiento de las mismas.

Por su parte, para efectos de la verificación del cumplimiento de la norma ISO existe el mecanismo de verificación de cumplimiento mediante la certificación, que para Colombia, como quedo dicho en apartes anteriores, entre otras organizaciones certificadoras de la ISO 27001, se encuentra el Icontec. Recuérdese que

> La **certificación** es el procedimiento mediante el cual un organismo da una **garantía** por escrito, de que un producto, un proceso o un servicio está **conforme a los requisitos especificados.**
>
> La certificación es en consecuencia el medio que está dando la garantía de la conformidad del producto a normas y otros documentos normativos. La certificación se materializa en un certificado: El **certificado** es un **documento** emitido conforme a las reglas de un **sistema de certificación,** que indica con un nivel suficiente de confianza, que un producto, proceso o servicio debidamente identificado, está conforme a una norma o a otro documento normativo especificado (Pons & Sivardière, 2002, pág. 12).

De lo anterior se deriva que para la norma ISO 27001 la autoridad estará radicada en los organismos de certificación, pues ellos dirán que tan conforme o no se encuentra una entidad en relación con el estándar planteado por la norma. La identificación de parte de la autoridad u organismo certificador de una no conformidad implicará una propuesta de mejora o incluso la no renovación de la condición de certificado. Pero en todo caso, no pasa de ser una afectación de valor agregado de la organización para efectos de su eficiente operación y/o su capacidad de competitividad.

Para el caso de las normas de la LEPD, como es sabido, no existe hoy en día en Colombia procesos de certificación de cumplimiento de sus obligaciones, lo que no significa que no existan autoridades de vigilancia de cumplimiento. Las funciones en esta materia están distribuidas según la naturaleza jurídica de la entidad. Si se trata de entidades públicas, las funciones de autoridad serán ejercidas por la Procuraduría General de la Nación conforme a lo ordenado en el parágrafo final del artículo 2.2.2.25.4.4 del Decreto 1074 de 2015. Cuando se refiere a una entidad privada la autoridad lo será la Superintendencia de Industria y Comercio, sobre la cual, en razón a su de-

pendencia política del Presidente de la República, y buscando su autonomía conforme a las exigencias de la OCDE, para el momento del presente trabajo, se está evaluando la designación por periodo (al parecer 4 años concomitante con el del presidente) para evitar su actual condición de libre nombramiento y remoción que puede poner en riesgo su independencia, máxime cuando está investido de funciones jurisdiccionales no obstante ser órgano administrativo.

Esta condición de elemento convergente se pone aún más de manifiesto con la noticia dada a conocer el pasado agosto de 2015, según la cual ya se inician los procesos de certificación de datos personales, tal vez como primera manifestación de implementación de sistemas de gestión de datos personales certificables conforme a normas corporativas vinculantes de las que trata el Decreto 1074 del 2015 en su artículo 2.2.2.25.6.2 y aún no desarrolladas en Colombia. El registro noticioso se dio a conocer en los siguientes términos:

> El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) reconoció a la Entidad Mexicana de Acreditación (EMA) como entidad de acreditación en materia de datos personales y la inscribió en el Registro de Esquemas de Autorregulación Vinculante (REA). El Sistema de Certificación en materia de protección de datos personales inició formalmente su operación, con el reconocimiento que recibió la EMA, por parte del INAI, como entidad de acreditación en la materia (Quadratin Mexico, 2015).

6.1.10 MECANISMOS DE SEGURIDAD SEGÚN CARACTERIZACIÓN DEL OBJETO REGLADO

Partiendo de la base de considerarse la información como el objeto reglado por la ISO 27001 y los datos respectivos de la LEPD, en tratándose de la primera, conforme lo señala en el numeral 6 (Icontec, 2013, p. 4) la categorización de la información resulta de interés en función de la criticidad de la misma, para resolver cuales han de ser los mecanismos de seguridad a adoptarse. En cuanto hace referencia a la segunda, conforme al artículo 2.2.2.25.6.1 del Decreto 1074 de 2015, los datos han de ser categorizados conforme al nivel de riesgo generado al titular del dato, para que con base en él, se adopten las medidas de seguridad apropiadas y efectivas para gestionar los riesgos a los que se exponen sus titulares. Es decir que, como elemento convergente entre las normas en análisis está la necesidad

de categorizar tanto la información como los datos y en función de ello determinar los mecanismos de aseguramiento a los que han de ser sometidos.

6.1.11 MANTENIMIENTO DEL SISTEMA

Finalmente, como último elemento convergente se ha identificado el riesgo de entropía tanto de la operación regulada por la ISO como del establecimiento de las condiciones de cumplimiento de la LEPD. En ambos casos se está implementando sistemas que, como tales, con el tiempo tienden a disminuir su dinámica, requiriendo por tanto de factores internos y externos que permitan la redinamización de los mismos. Esto se logra a través de los sistemas de auditoría. Su revisión periódica, el detectar sus hallazgos, el efectuar su correspondiente plan de mejora continua y por lo tanto la supervisión del cumplimiento de las recomendaciones, constituye la energía interna y externa que requieren los sistemas para asegurar su supervivencia adecuada a los propósitos que motivan su implantación, exigibilidad que vuelve a repetirse, lo demandan por igual los SGSI reglados por la norma ISO, como los SGSDP que han de implantarse conforme a la LEPD.

6.2 **ELEMENTOS DIVERGENTES**

Así como se identifican aspectos convergentes entre la NTC/ISO/IEC 2701:2013 y la LEPD, también hay algunos aspectos divergentes que explican entre otras por qué, como se ha observado en la práctica, una organización que se ha certificado en ISO 27001, no obstante que el control A.18.1.4 del área de cumplimiento de la mencionada norma es justamente privacidad y protección de información de datos personales, no necesariamente se encuentra cumpliendo la LEPD. Esta circunstancia es justamente el objetivo de las líneas que siguen en el presente trabajo, con la advertencia igual efectuada sobre los aspectos convergentes, en cuanto que no son de seguro los únicos, pero si los identificados como más relevantes por quien presenta este trabajo.

6.2.1 VALORACIÓN DEL OBJETO DE ASEGURAMIENTO

Tal vez el elemento más significativo y que marca una lógica muy propia de cada una de las normas en análisis, lo constituye el elemento de valoración del objeto de aseguramiento de cada una de ellas.

Recuérdese que el objeto de aseguramiento para la ISO lo es la información como un activo de la organización. Es decir que la información es vista como un bien económico en cuanto que, creado por el hombre posee un propietario que, en razón de su valor económico y su valor de uso, puede transarlo. Podría decirse que el propietario de una organización que, como es obvio, maneja información, así como en principio es dueño de la máquina de producción, también lo es de aquella que circula en su empresa. Podrá, por tanto, disponer libremente de todo ello como bienes que configuran su patrimonio, obvio siempre en el marco de la ley.

Por otra parte, el objeto de aseguramiento para la LEPD lo es el dato personal entendida como la huella virtual de la naturaleza humana. Somos en la medida de nuestros datos, podría decirse. Por ello los datos personales, si bien es cierto son una creación cultural, científica, sociológica, tecnológica, etc. del ser humano, no le pertenecen sino al respectivo titular, careciendo por tanto en sí mismo de valor económico. En principio, resulta imposible económicamente hablando transferir la propiedad del nombre, la huella digital, la estructura del iris, el número de la identificación, etc. Sus características están hatadas a la naturaleza y la existencia humana y de contera amalgamados al principio de dignidad expresado en los capítulos introductorios de este trabajo. Por ello, si dentro de la información de una organización se tratan datos personales, estos no podrán ser considerados como un bien más de los varios de propiedad del dueño de aquella. El real propietario lo será el titular y, conforme a la autorización y la finalidad de su recolección deberá darle el tratamiento correspondiente. De ello se deriva que el propietario de la organización que trata datos personales, ya sea como Responsable o como Encargado, es en realidad un albacea de una extensión particular del ser humano, sus singularidades, también llamadas datos personales. Es decir que, de lo dicho cabe decir en consecuencia que la valoración del objeto de la ISO 27001 es fundamentalmente económico, en tanto que la valoración del objeto de la LEPD es esencialmente moral.

6.2.2 OBLIGATORIEDAD DE LA NORMA

Otro aspecto claramente divergente es la naturaleza coercitiva o no de las disposiciones en análisis. Mientras la implementación de la NTC/ISO/IEC 27001:2013 es por regla casi generalísima una decisión sujeta a la mera liberalidad de la organización, efectuada con miras al mejoramiento de la operación y a la protección de activos, tal como quedo dicho, la LEPD es por regla generalísima una obligación de naturaleza legal que se impone a todas y cada una de las organizaciones públicas o privadas que traten datos personales ya sea como responsable o como encargados o subencargados. La no implementación de la norma ISO, salvo excepciones muy escasas como las referidas en relación con la operación del sistema PILA en Colombia, no acarreará para la organización más que pérdida de competitividad y obviamente aumento de riesgos. En cambio, la no implementación de la LEPD además de las anteriores consecuencias, puede implicar sanciones por parte de la autoridad tales como la suspensión de la utilización de la base de datos, multas hasta de 1000 salarios mínimos mensuales legales vigentes, dependiendo de las circunstancias incluso responsabilidad penal, etc.

6.2.3 PRINCIPIOS DIFERENCIADORES

Basado en el anterior aspecto, no obstante haber sido identificado como convergente el hecho de estar regladas las normas en cotejo por principios, se identificó una clara diferenciación en cuanto a la aceptación o no de los principios basados en valores humanistas. Recuérdese que, como quedó descrito, la ISO hace exclusión, justamente de dos principios de gestión de seguridad de los propuestos por la OCDE que tienen tal contenido valorativo, esto es el Principio de Moralidad y el Principio de Democracia. En cambio, por su parte la LEPD tiene incorporado como valor, como principio y como regla, justamente la Dignidad Humana obligando como lo señaló la jurisprudencia que siempre que se esté frente al tratamiento de los datos, ello debe hacerse bajo el entendimiento del marco normativo de los derechos fundamentales.

6.2.4 DOCUMENTACIÓN DIFERENCIADA

Claro resulta que, si los principios, los objetos y factores de valoración de los mismos, así como los objetivos de cada una de las nor-

mas son diferentes, se dé el evento de exigencias de soportes documentales que son solo del ámbito de cada una de ellas.

Por los propósitos de este trabajo, se enuncian algunos de los registros documentales que, como resulta obvio, son exigidos por la LEPD para efectos de la *accountability* y no así por la ISO en referencia.

> Registro de Autorizaciones de Titulares. Busca llevar el archivo de todas y cada una de las autorizaciones que los titulares de datos han dado al Responsable y/o Encargado, para el evento en que sea requerida por estos o por las autoridades de control y vigilancia.
>
> Registro de Publicación de Avisos de Privacidad. Por existir la obligación de efectuar el aviso de privacidad justamente para efectos de dar a conocer la PTI que la alta dirección encargada de ello aprobará, debe conservarse tanto el aviso como los registros de los mecanismos usados para efectos de dar a conocer aquella, es decir, publicaciones de prensa, subidas en páginas web, correos enviados, etc.
>
> Registro de PQR y de supresión de datos. Para la LEPD la atención de los titulares es aspecto de suma importancia, sumado a cualquier tipo de relacionamiento que una autoridad o incluso un tercero desee efectuar con los datos que trata la organización. Por ello se debe llevar un registro de las peticiones o quejas que en relación con los datos se efectúen. De hecho muchas de las sanciones que a la fecha ha impuesto la SIC en el caso colombiano, están asociadas al tema de la atención de PQR, que entre otras posee una reglamentación especial diferente a la regla general de atención de derechos de petición que el Código de Procedimiento Administrativo y de lo Contencioso Administrativo –CPACA– regula y que ha sido adoptado por la mayoría de las organizaciones para atender el tema de derechos de petición relacionados con datos personales, perdiendo de vista la exigencia particular de la LEPD y las responsabilidades que se derivan de su incumplimiento.

6.2.5 EXIGIBILIDAD DE REGISTRO EXTERNO

En tratándose de la información bajo la lógica de la norma ISO 27001, no se ha establecido requisito alguno que establezca la obligación de inscribir ante ningún organismo las bases de datos de la información que se gestiona al interior de la organización. Su manejo, ubicación, accesos, etc., está sometido solo al arbitrio de la organización misma. En tanto que para la LEPD si se ha establecido por mandato del Decreto 1074 de 2015 reglamentario de la Ley 1581 de 2012, que las bases de datos físicas y digitales que contienen datos personales, deben ser reportados a la SIC mediante la inscripción de dichas bases en el RNBD.

7. CONCLUSIONES

Dentro de las varias conclusiones que pueden derivarse del ejercicio desarrollado a lo largo del trabajo que en el presente documento se entrega, se pueden extraer las siguientes:

1. El trasplante normativo efectuado con la Ley 1581 de 2012 (LEPD), ha implicado la tropicalización de las normas europeas y en especial de la LOPD de España, con ciertas particularidades que generan, cuando no vacíos normativos graves, si claras incoherencias, por ejemplo con la reglamentación de la transferencia internacional de datos o la clasificación que se ha planteado de los datos mismos, circunstancias que obligan de la autoridad forzadas interpretaciones legales, las que exponen injustificadamente a las organizaciones a sanciones.

2. El proceso de desarrollo del Hábeas Data en Colombia, y por tanto su decantación dogmática, aún está en ciernes. Temas esenciales como la responsabilidad contractual por el incumplimiento de las obligaciones nacidas del contrato principal o accesorio de tratamiento de datos personales, aún no ha sido desarrollado, igual que ocurre con la responsabilidad extracontractual por daños causados con ocasión del tratamiento de datos personales por orden legal o judicial.

3. Las orientaciones dadas por la Superintendencia de Industria y Comercio a efectos de lograr el cumplimiento por parte de los obligados de la LEPD, como por ejemplo la guía *de accountability* y el manual de RNBD, permiten identificar que detrás de la normativa nacional está como soporte teórico conceptual la norma NTC/ISO/IEC 27001:2013.

4. La LEPD y la NTC/ISO/IEC 27001:2013, son ambas fruto de trasplantes normativos desde el núcleo del pensamiento europeo hacia América Latina y en especial Colombia, auspiciado, cuando no acompañado, por la OCDE como organismo multilateral de unificación de exigencias para facilitar el intercambio económico transfronterizo.

5. La identificación de los elementos convergentes entre la NTC/ISO/IEC 27001:2013 y la LEPD, pone de presente que, aun cuando son universos de regulación diversos para nada son excluyentes y, por

el contrario, frente a los vacíos legales la primera coadyuva cuando de buscar la conformidad con la ley se trata, sin perjuicio de las ciertas áreas propias donde se ubican los elementos divergentes, tal como se grafica en la siguiente figura:

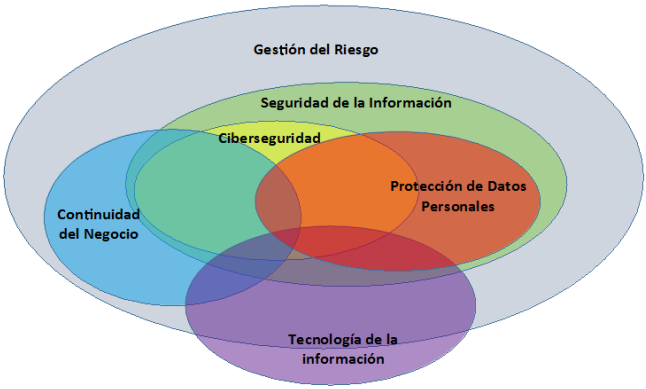


Figura 24. *Imagen de correlación de los SGSI y SGSDP*

Fuente: (basado en la gráfica de venn de Kosutic).

«La intervención al interior de una organización para efectos del cumplimiento de la ley de Hábeas Data, implica relacionamiento con las áreas de la Continuidad del Negocio, Ciberseguridad, Gestión de Infraestructura de TIC, todo en el marco de la gestión de la seguridad de la información.»

6. La gestión de los datos personales, como información que lo es, para su tratamiento requiere una sabia armonización entre humanismo y utilitarismo. Ello por cuanto que, mientras el universo de aplicación de la LEPD tiene que ser abordado siempre en función de la dignidad humana y de los derechos fundamentales, el de la aplicación de la NTC/ISO/IEC 27001:2013 ha de desarrollarse en relación costo beneficio entre el valor de la información y los requerimientos para su custodia.

7. Así como la NTC/ISO/IEC 27001:2013 se materializa al interior de las organizaciones mediante el diseño e implementación de un Sistema de Gestión de Seguridad de la Información –SGSI–, para lograr el adecuado cumplimiento de la LEPD deberá diseñarse e implementarse también un Sistema de Gestión de la Seguridad de los Datos Personales SGSDP, constituyendo la primera, por razón de los ele-

mentos comunes que le relacionan con la segunda, una base importante para su desarrollo.

8. La falta en Colombia de un SGSDP acorde a la LEPD que permita la certificación del cumplimiento, afecta el principio de confianza legítima por la incertidumbre que genera a las organizaciones dimensionar las «medidas apropiadas y efectivas» exigidas por la ley para el cumplimiento del principio de responsabilidad demostrada o *accountability*.

9. Así como la NTC/ISO/IEC 27001:2013 se materializa al interior de las organizaciones mediante el diseño e implementación de unos sistemas de gestión de seguridad de la información –SGSI–, para lograr el adecuado cumplimiento de la LEPD deberá diseñarse e implementarse también un sistema de gestión de la seguridad de los datos personales SGSDP.

10. No necesariamente la implementación de un SGSI presupone el cumplimiento de las exigencias de la LEPD, como tampoco el cumplimiento de la LEPD mediante la implementación de un SGSDP presupone que la organización esté lista para ser certificada en la norma NTC/ISO/IEC 27001:2013.

11. En el evento en que un juez requiera definir si una organización se encuentra cumpliendo o no las exigencias de la LEPD, podrá apalancarse en la NTC/ISO/IEC 27001:2013 a efectos de identificar, con base en los elementos convergentes, si los mecanismos implementados por ella fueron o no los apropiados y efectivos para proteger a los titulares. De igual manera, la relación entre ellas le facilita al juzgador un puente de interpretación jurídica en el marco de los ambientes globalizados, dadas las relaciones transfronterizas que pueden alcanzar los intercambios de datos.

8. REFERENCIAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2014). *www.agpd.es*. Recuperado el 4 de 5 de 2015, de Agencia Española de Protección de Datos Personales: https://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/oposicion-ides-idphp.php

AGPD (2013). *Agencia Española de Protección de Datos*. Recuperado el 19 de Junio de 2015, de www.agpd.es: http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/Paises_autoridad_Proteccion_Datos_Miembro_Conferencia_Internacional.pdf

AKITSUKI, Y., y DECETY, J. (2013). *El contexto social y la egencia percibida afecta empatía por el dolor: Una investigación FMRI relacionados con el evento*. Universidad de Chicago, Departamento de Psicología y Psiquiatría, y el Centro de Neurociencia Cognitica y Social, Chicago.

ALEKOS, J. (6 de 3 de 2015). Recuperado el 2 de 5 de 2015, de periodismohumano.com: http://periodismohumano.com/economia/cronica-de-una-detencion-documentada-periodista-freejaimealekos.html

AQUINO, T. (marzo de 2001). *Suma Teológica-Santo Tomás de Aquino*. Recuperado el 22 de 12 de 2014, de http://biblioteca.campusdominicano.org/1.pdf: http://biblioteca.campusdominicano.org/1.pdf

ARANGO RIVADENEIRA, R. (2012). *El concepto de derechos sociales fundamentales* (segunda edición complementada ed.). Bogotá D. C., Colombia: Legis Editores S. A.

ARISTÓTELES. (2005). *La República*. (P. López Barja de Quijano, y E. García Fernández, Edits.). Madrid, Espala: Ediciones Istmo S. A.

BUENO, C. (21 de enero de 2015). *http://www.eleconomista.es*. Recuperado el 24 de agosto de 2015, de elEconomista.es: http://www.eleconomista.es/telecomunicaciones-tecnologia/noticias/6407837/01/15/Los-ciberataques-a-gobiernos-empresase-instituciones-desafian-el-orden-mundial-.html

CAMPDERRICH BRAVO, R. (2007). *Cuadernos electrónicos de filosofía del derecho 15*. Recuperado el 6 de 9 de 2014, de http://www.uv.es/CEFD/15/Campderrich.pdf: http://www.uv.es/CEFD/15/Campderrich.pdf

CAPURRO, R. (abril de 2007). *Serbiluz-Sistema de servicios bibliotacarios y de información*. Recuperado el 24 de septiembre de 2015, de www.produccioncientificaluz.org/: http://www.produccioncientificaluz.org/index.php/enlace/article/view/13372/13357

CERDA SILVA, A. (2003). *Revista Chilena de Derecho Informático*. Recuperado el 16 de febrero de 2015, de http://web.uchile.cl: http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_complex/0,1491, SCID%253D14331%2526ISID%253D507,00.html

CERDA SIVA, A. (2006). *Ius et Praxis versión Online*. Recuperado el 7 de 3 de 2015, de www.scielo.cl: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122006000200009

COELLO, H. (9 de octubre de 2009). *https://helkyncoello.wordpress.com*. Recuperado el 14 de julio de 2015, de Helkyn Coello Blog: https://helkyncoello.wordpress.com/category/gobierno-de-ti/

CONGRESO DE LOS ESTADOS UNIDOS (1974). *USA Deparment of Estate Freedom of Informetion Act*. Recuperado el 7 de 3 de 2015, de foia.state.gov: http://foia.state.gov/Learn/PrivacyAct.aspx

CONSEJO DE LA UNIÓN EUROPEA (11 de junio de 2015). *European Council-Council of the European Union*. Recuperado el 1 de octubre de 2015, de http://data.consilium.europa.eu/: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/es/pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL DE LA REPÚBLICA DE COLOMBIA (14 de julio de 2011). *Ministerio de las TIC*. Recuperado el 17 de septiembre de 2015, de /www.mintic.gov.co: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

COTE URIBE, G. (1981). *López Michelsen presidente 1982: la respuesta del liberalismo al chantaje de las derechas*. Bucaramanga: Nueva Jornada.

CSO ESPAÑA-COMPUTERWORLD (16 de junio de 2015). *cso.computerworld.es*. Recuperado el 12 de septiembre de 2015, de CS España-Computerwordl: http://cso.computerworld.es/seguridad-en-cifras/el-coste-de-las-brechas-de-datos-superara-los-21-billones-de-dolares-en-2020

DARWIN, C. (1852). *Fondo Digitalizados de la Universidad de Sevilla*. Recuperado el 2 de febrero de 2015, de fondosdigitales.us.es: http://fondosdigitales.us.es/fondos/libros/3247/15/la-expresion-de-las-emociones-en-el-hombre-y-en-los-animales/

DE ROUX-RENGIFO, S. F. (2009). *Scielo-Cuadernos de Contabilidad* (Scielo.org, Ed.) Recuperado el 31 de enero de 2014, de http://www.scielo.org.co: http://www.scielo.org.co/scielo.php?pid=S0123-14722009000200008&script=sci_arttext&tlng=en

DELGADO PARRA, M. (2001). *www.filosofia.net/*. Recuperado el 6 de 9 de 2014, de www.filosofia.net/: http://www.filosofia.net/materiales/num/num14/n14d.htm#_ftn33

DEPARTAMENT OF DEFENSE-USA. (15 de agosto de 1983). *National Intitute of Standars and Technology.* Obtenido de www.csrc.nist.gov: http://csrc.nist.gov/publications/history/dod85.pdf

DEPARTAMENTO DE DERECHO INTERNACIONAL DE LA SECRETARÍA DE ASUNTOS JURÍDICOS (17 de octubre de 2011). *Organización de Estados Americanos*. Recuperado el 5 de agosto de 2015, de www.oas.org: http://www.oas.org/dil/esp/CP-CAJP-2921-10_rev1_corr1_esp.pdf

DWORKIN, R. (1984). *www.uruguayeduca.edu.uy.* Recuperado el 6 de agosto de 2014, de http://www.uruguayeduca.edu.uy/Userfiles/P0001/File/El%20modelo%20de%20las%20normas.pdf.

— (2012). *Una cuestión de principios.* Buenos Aires, Argentina: Siglo XXI Editores S. A.

ESPINOZA MAESTRE, F. (2005). «Agosto de 1936. Terror y propaganda. Los orígenes de la Causa General» (U. D. Contemporánea, Ed.) *Pasado y Memoria. Revista de Historia Contemporánea,* 4, 15-26.

FROMM, E. (1964). *Psicoanálisis de la sociedad contemporánea* (6.ª edición). (F. d. Económica, Ed.) Buenos Aires, Mexico.

GAMMA SSL (2014). *Gamma Secure Systems Limited.* Recuperado el 4 de agosto de 2015, de www.gammassl.co.uk: http://www.gammassl.co.uk/27001/history.php

GARCÍA GARCÍA, L. (2011). «Bartolomé de las Casas y los Derechos Humanos». En L. Méndez Francisco, *Derechos humanos en su origen: La Republica Dominicana y Antonio Montesinos* (págs. 81-114). Salamanca, España: San Esteban.

GLOBAL STD (23 de septiembre de 2013). *Global STD-Certificación.* Recuperado el 10 de septiembre de 2015, de Global STD: http://www.globalstd.com/networks/blog/estadisticas-de-certificados-iso-2013

GOBIERNO DE ESPAÑA-MINISTERIO DE EDUCACIÓN (2015). *didacTerion: Utilidades para el desarrollo de contenidos educativos interactivos.* Recuperado el 23 de 3 de 2015, de www.didacterion.com: http://www.didacterion.com/esddlt.php

GURRÍA, J. Á. (7 de 3 de 2015). *Portafolio Economía.* Recuperado el 7 de 3 de 2015, de www.portafolio.co: http://www.portafolio.co/economia/ingreso-colombia-la-ocde-2016

HANSON, K., y Ceppos, J. (6 de 10 de 2006). *http://www.scu.edu/ethics/.* (S. C. University, Productor) Recuperado el 1 de 5 de 2015, de Markkula Center for Applied Ethics: http://www.scu.edu/ethics/publications/ethicalperspectives/leaks.html

HEREDERO MANUEL, H. (27 de abril de 2011). *www.mjusticia.gob.es.* Recuperado el 7 de 3 de 2015, de http://www.mjusticia.gob.es/cs/Satellite/1292344070195?blobheader=application%2Fpdf&blobheadername1=Content..)

HUSTINX, P. (26 de 3 de 2014). *Resumen ejecutivo del dictamen preliminar del Supervisor Europeo de Protección de Datos sobre Intimidad y competitividad en la era de la obtención de datos masivos.* (http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:JOC_2014_225_R_0007#ntc4-C_2014225ES.01000601-E0004, Ed.) Recuperado el 18 de 07 de 2014, de www.eur-lex.europa.eu: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=OJ:JOC_2014_225_R_0007#ntc4-C_2014225ES.01000601-E0004

ICONTEC. (2013). *Norma Técnica NTC/ISO/IEC 27001-2013-12-11 - Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos*. Bogotá D. C.: Icontec.

— (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27001*. Bogotá, Colombia: ICONTEC.

INAI (noviembre de 2014). *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*. Obtenido de http://inicio.ifai.org.mx: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa%20implementaci%C3%B3n%20SGSDP%20-%20Noviembre2014.pdf

INCODER (5 de marzo de 2013). *INCODER-Instituto Colombiano de Desarrollo Rural*. Recuperado el 16 de enero de 2015, de www.incoder.gov.co: http://www.incoder.gov.co/documentos/A%C3%91O_2013/Normatividad/Resoluciones/Res_0314_de_05_MAR_2013.pdf

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (marzo de 2014). *www.ifai.org.mx*. Recuperado el 8 de junio de 2015, de Ifai: http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Riesgo_BAA_marzo2014.pdf

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, ANTES IFAI (17 de julio de 2009). *INAI*. Recuperado el 19 de mayo de 2015, de www.ifai.org.mx: http://inicio.ifai.org.mx/DocumentosdeInteres/guia_elaboracion_documento_seguridad_1_4.pdf

ISO-ONUDI (febrero de 2010). *ISO*. Recuperado el 27 de septiembre de 2015, de www.iso.org: http://www.iso.org/iso/fast_forward-es.pdf

ISO (febrero de 2010). *Organización Internacional de Normalización-ISO*. Recuperado el 26 de septiembre de 2015, de www.iso.org: http://www.iso.org/iso/private_standards-ES.pdf iso27000.es. (2005). *ISO27000. ES*. Recuperado el 26 de septiembre de 2015, de iso27000.es: iso27000.es/iso27002_8.html

ISO27000.es (2012). *ISO 27000.es El portal de ISO 27001 en Español*. Recuperado el 7 de enero de 2015, de www.iso27000.es: http://www.iso27000.es/iso27000.html

— (2012). *ISO27000. ES*. Recuperado el 20 de septiembre de 2015, de El portal de ISO 27001 en español: http://www.iso27000.es/sgsi.html

JUAN PABLO II (1 de septiembre de 2011). *Vida Humana Internacional*. Recuperado el 2 de febrero de 2015, de http://vidahumana.org: http://vidahumana.org/vida-humana-internacional/item/866-carta-apost%C3%B3lica-mulieris-dignitatem-del-sumo-pont%C3%ADfice-juan-pablo-ii-sobre-la-dignidad-y-la-vocaci%C3%B3n-de-la-mujer-con-ocasi%C3%B3n-del-a%C3%B1o-mariano

K. S. TONG, C., y T. T. WONG, E. (2008). *Governance of Picture Archiving and Communications Systems: Data Security and Quality Management of Filmless Radiology*. Nueva York, Hershey, Estados Unidos: IGI Global. doi:10.4018/978-1-59904-672-3

KOSUTIC, D. (13 de septiembre de 2010). *Advisera*. Recuperado el 21 de septiembre de 2015, de http://advisera.com: http://advisera.com/27001academy/es/blog/2010/09/13/iso-27001-vs-iso-27002-2/

— (2012). *Ciberseguridad en 9 pasos-El manual sobre seguridad de la información para el gerente*. (http://advisera.com/27001academy/es/books/ciberseguridad-en-9-pasos-el-manual-sobre-seguridad-de-la-informacion-para-el-gerente/, Ed., & G. Trentini, Trad.) Electrónico: EPPS Services Ltd, Zagreb.

LÓPEZ MEDINA, D. E. (2012). *El derecho de los Jueces-Obligatoriedad del precedente constitucional, análisis de sentencias y líneas jurisprudenciales y teoría del derecho judicial* (segunda edición 2006, Undécima reimpresión 2012 ed.) (Universidad de los Andes, Ed.). Bogotá: Legis Editores S. A.

MARSHALL, G. C. (5 de 6 de 1947). *OCDE Home*. Recuperado el 7 de 3 de 2015, de http://www.oecd.org/: http://www.oecd.org/general/themarshallplanspeechatharvarduniversity5june1947.htm

MINISTERIO DE ASUNTOS EXTERIORES Y COOPERACIÓN, G. D. (5 de mayo de 1949). *Gobierno de España*. Recuperado el 19 de febrero de 2015, de http://www.exteriores.gob.es/Portal/es/Paginas/inicio.aspx: http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/ConsejoDeEuropa/Paginas/HistoriaActividadConsejoEuropa.aspx

MINISTERIO DE LA DEFENSA NAL.-DIRECCIÓN DE ESTUDIOS SECTORIALES-DIRECCIÓN DE PROGRAMAS (octubre de 2009). *http://www.mindefensa.gov.co*. Recuperado el 18 de agosto de 2015, de http://www.mindefensa.gov.co: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

MINISTERIO DE LAS TIC DE COLOMBIA (8 de enero de 2015). *MINTIC*. Recuperado el 21 de septiembre de 2015, de www.mintic.gov.co: http://www.mintic.gov.co/gestionti/615/articles-5482_Controles.pdf

— (30 de junio de 2011). *Gobierno en Línea*. Recuperado el 14 de enero de 2015, de http://viejoprograma.gobiernoenlinea.gov.co/: http://viejoprograma.gobiernoenlinea.gov.co/apc-aa-files/Presentaciones/Manual_GEL_V3_0__VF.pdf

MINISTERIO DE RELACIONES EXTERIORES (15 de noviembre de 2011). *Cancillería*. Recuperado el 15 de enero de 2015, de www.cancilleria.gov.co/: http://www.cancilleria.gov.co/sites/default/files/estudios_previos_19.pdf

MOCHAL, T. (18 de diciembre de 2006). *2015 CBS Interactive. TechRepublic ZDnet*. Recuperado el 11 de junio de 2015, de ZDnet: http://www.techrepublic.com/article/fast-tracking-and-crashing-can-get-your-project-back-on-schedule/

MUÑOZ PERIÑÁN, I., y ULLOA VILLEGAS, G. (2011). Recuperado el 10 de septiembre de 2015, de www.icesi.edu.co: https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/viewFile/1052/1076

OBAMA, B. (12 de diciembre de 2013). *http://caracol.com.co*. Recuperado el 10 de marzo de 2014, de Caracol Radio: http://caracol.com.co/radio/2013/12/11/internacional/1386723840_035114.html

OCDE (1980). *IFAI*. Recuperado el 5 de noviembre de 2014, de inicio.ifai.org.mx: inici.ifai.org.mx/DocumentosdeInteres/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad.pdf

— (25 de julio de 2002). *OCDE*. Recuperado el 27 de septiembre de 2015, de www.oecd.org: http://www.oecd.org/sti/ieconomy/34912912.pdf

OEA, S. S. (junio de 2014). *http://www.symantec.com/*. Recuperado el 24 de agosto de 2015, de Symantec: http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

OEHLING DE LOS REYES, A. (2010). La dignidad de la persona. Evolución histórico-filosófica, concepto, recepción constitucional y relación con los valores y derechos fundamentales. 284-308.

OFICINA DE PUBLICACIONES OFICIALES DE LAS COMUNIDADES EUROPEAS (2000). *Diálogo con los ciudadanos y las empresas-Europa en directo*. Recuperado el 8 de febrero de 2014, de ec.europa.eu: http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-spain_es.pdf

OIT (1977). *Organización Internacional del Trabajo*. Recuperado el 13 de agosto de 2015, de www.ilo.org/: http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_112625.pdf

ONAC (2010). *Organismo Nacional de Acreditación*. Recuperado el 20 de enero de 2015, de www.onac.org.co: http://www.onac.org.co/modulos/contenido/default.asp?idmodulo=252

ORGANIZACIÓN MUNDIAL DE COMERCIO –OMC– (2014). *World Trade Organization*. Recuperado el 12 de septiembre de 2015, de www.wto.org: https://www.wto.org/spanish/res_s/publications_s/tbttotrade_s.pdf

ORWELL, G. (1984). *1984* (R6 08/01 ed.). (E. E. http://biblio3.url.edu.gt/Libros/2011/1984.pdf, Ed., y R. V. Zamora, Trad.) Salvat Editores S. A. Obtenido de biblio3.url.edu.gt: http://biblio3.url.edu.gt/Libros/2011/1984.pdf

OZORES, P. (30 de 1 de 2015). *Tecnología Regional*. Recuperado el 8 de 3 de 2015, de www.bnamericas.com: http://www.bnamericas.com/news/tecnologia/bajo-la-lupa-el-proyecto-de-proteccion-de-datos-de-brasil

PALLAS MEGA, G. (diciembre de 2009). *Facultad de Ingeniería-Universidad de la República de Uruguay*. Recuperado el 29 de septiembre de 2015, de www.fing.edu.uy: https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

PELÉ, A. (2004). *Una aproximación al concepto de dignidad*. Recuperado el 6 de agosto de 2014, de www.revistauniversitas.org: http://universitas.idhbc.es/n01/01_03pele.pdf

— (2010). *La Dignidad Humana. Sus orígenes en el pensamiento clásico*. (N. D. Madrid, Ed.) Madrid, España: Editorial Dykinson.

PIÑAR MAÑAS, J. L. (28 de octubre de 2009). *http://www.falternativas.org*. Recuperado el 24 de enero de 2015, de Fundación Alternativas: http://www.falternativas.org/laboratory/documentos/documentos-de-trabajo/seguridad-transparencia-y-proteccion-de-datos-el-futuro-de-un-necesario-e-incierto-equilibrio

PONS, J.-C., y SIVARDIÈRE, P. (2002). *Organización de las Naciones Unidas para la Alimentación*. (M. T. Tartanac, Ed.) Recuperado el 2 de octubre de 2015, de www.fao.org: http://www.fao.org/docrep/004/ad094s/ad094s03.htm

PORTALWEB AGPD. (2001). *Agencia Española de Protección de Datos –AGPD–*. Recuperado el 7 de 8 de 2015, de www.agpd.es: https://www.agpd.es/portalwebAGPD/internacional/adecuacion/estados_unidos/common/pdfs/ElAcuerdodePuertoSeguroconlosEstadosUnidos.pdf

PRENSA LATINA-AGENCIA INFORMATIVA LATINOAMERICANA-LP (21 de septiembre de 2014). *http://lagazzettadf.com*. Recuperado el 13 de junio de 2015, de La Gazzetta DF: http://lagazzettadf.com/noticia/2014/09/21/reportan-altos-indices-de-ciberataques-en-mexico/

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA (abril de 2015). *Presidencia de la República*. Recuperado el 28 de septiembre de 2015, de wp.presidencia.gov.co: http://wp.presidencia.gov.co/sitios/dapre/sigepre/guias/G-GD-02%20Gu%C3%ADa%20para%20la%20Clasificaci%C3%B3n%20de%20la%20Informaci%C3%B3n.pdf

QUADRATIN MEXICO (1 de agosto de 2015). *Quadratin Mexico*. Recuperado el 6 de agosto de 2015, de www.mexico.quadratin.com.mx: https://mexico.quadratin.com.mx/Inicia-operacion-Sistema-de-Certificacion-de-proteccion-de-datos/

REAL ACADEMIA ESPAÑOLA (2012). *Real Academia Española*, 22. Recuperado el 6 de 8 de 2014, de www.rae.es: http://lema.rae.es/drae/?val=dignidad

— (2012). *Real Academia Española*, 22. Recuperado el 6 de agosto de 2014, de www.rae.es: http://lema.rae.es/drae

— (2014). *Real Academia Española*. Obtenido de www.lema.rae.es/: http://lema.rae.es/drae/?val=informaci%C3%B3n

REBOLLO DELGADO, L. (2014). *ProQuest ebrary.* (Dykinson, Ed.) Recuperado el 19 de febrero de 2015, de http://site.ebrary.com/: http://site.ebrary.com/lib/bibliotecaustasp/reader.action?docID=10903674&ppg=140

RIQUELME, U. H. (2004). La medicina bajo el nazismo: una aproximación histórica cultural. Segunda Parte. (U. P. Bolivariana, Ed.) *Medicina UPB, 23*(1), 25-27.

ROUSSEAU, J. J. (1999). *www.enxarxa.com*. Recuperado el 2 de agosto de 2014, de http://www.enxarxa.com/biblioteca/ROUSSEAU%20El%20Contrato%20Social.pdf.

SAARENPÄÄ, A. (diciembre de 2003). *Revista Chilena de Derecho Informático No. 3*. Recuperado el 12 de julio de 2014, de http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492, SCID%253D14232%2526ISID%253D507,00.html

SALCEDO B., R. J. (19 de diciembre de 2014). *Universidad Oberta de Cataluña*. Recuperado el 1 de octubre de 2015, de http://openaccess.uoc.edu: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/41002/4/rsalcedobTFC-1214memoria.pdf

SÁNCHEZ PÉREZ, G., y ROJAS GONZÁLEZ, I. (5 de junio de 2012). *Revista. Seguridad*. Recuperado el 7 de 2 de 2014, de http://revista.seguridad.unam.mx: http://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93

SARAVIA, G. (enero de 2012). *Universitas. Revista de Filosofía, Derecho y Política*. Obtenido de http://universitas.idhbc.es/n15/15-07.pdf

SEMANA (16 de junio de 2015). *Semana*. Recuperado el 17 de septiembre de 2015, de http://www.semana.com: http://www.semana.com/tecnologia/articulo/que-tan-preparado-esta-el-gobierno-contra-ataques-ciberneticos/431602-3

SERPA URIBE, H. (2009). *Constitución Política de Colombia-18 años* (primera ed.). Bogotá, Colombia: Legis S. A.

STALLING, W. (23 de agosto de 2004). *Universidad Tecnológica de Izúcar de Matamoros* (segunda edición ed.). Madrid, España: Pearson Prentice Hall. Recuperado el 25 de septiembre de 2015, de www.utim.edu.mx: http://www.utim.edu.mx/~svalero/docs/Antologia%20Seguridad%20de%20la%20Informacion.pdf

— (23 de agosto de 2004). *Fundamento de Seguridad en Redes, Aplicaciones y Estándares* (segunda edición ed.). Madrid: Pearson Educación, S. A. Recuperado el 25 de septiembre de 2015, de www.utim.edu.mx: http://www.utim.edu.mx/~svalero/docs/Antologia%20Seguridad%20de%20la%20Informacion.pdf

STEWART, D. (9 de marzo de 2012). *Organitation of American States*. Recuperado el 16 de 5 de 2015, de http://www.oas.org: http://www.oas.org/es/sla/cji/docs/CJI-doc_402_12_rev2.pdf

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO (3 de noviembre de 2015). *Circular Externa No. 2*. Recuperado el 10 de 3 de 2016, de http://www.sic.gov.co/drupal/recursos_user/documentos/normatividad/circular/2015/Circular_02.pdf

— (28 de mayo de 2015). *Superintendencia de Industria y Comercio*. Recuperado el 19 de junio de 2015, de www.sic.gov.co: http://www.sic.gov.co/drupal/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada

— (2 de octubre de 2015). *Superintendencia de Industria y Comercio*. Recuperado el 2 de octubre de 2015, de www.sic.gov.co: http://www.sic.gov.co/drupal/registro-nacional-de-bases-de-datos

SUPERINTENDENCIA FINANCIERA DE COLOMBIA (25 de octubre de 2007). *Enlace Operativo*. Recuperado el 15 de enero de 2015, de www.enla-

ceoperativo.com: http://www.enlaceoperativo.com/images/documentos/CircularExterna052_07.pdf

TAGORE, R. (2002). *http://www.cetr.net*. Recuperado el 24 de enero de 2015, de http://www.cetr.net/modules.php?name=News&file=article&sid=874

TEJERINA RODRÍGUEZ, O. (2014). *Seguridad del Estado y privacidad*. Madrid, España: Editoiral Reus.

THE GUARDIAN (15 de 2 de 2015). *www.theguardian.com*. Recuperado el 1 de 5 de 2015, de Theguardian: http://www.theguardian.com/us-news/2015/feb/02/fbi-anonymous-hacktivist-jeremy-hammond-terrorism-watchlist

TORRALBA I ROSELLÓ, F. (2005). «La raíz de la dignidad humana. Apostillas filosóficas a Francis Fukuyama». En J. Masiá Clavel, y E. D. Brouwer (Ed.), *Ser Humano, persona y dignidad* (págs. 244-262). España: Declée de Brower. Recuperado el 31 de julio de 2014, de www.ebrary.com: http://site.ebrary.com/lib/bibliotecaustasp/docDetail.action?docID=10526886

TRIBUNAL DE JUSTICIA (Gran Sala). (7 de octubre de 2015). *Fersaco S. A. S.* Recuperado el 7 de octubre de 2015, de Fersaco S. A. S.: http://www.fersaco.com/

TRUJILLO MARIEL, P. (2009). *Poder, sociedad y estructura: una mirada al dolor desde la perspectiva social*. Ciudad de Mexico, Mexico: Alfil, S. A. de C. V?

ÚBEDA DE TORRES, A. (2006). *Democracia y derechos humanos en Europa y en América. Estudio comparado de los sistemas europeo e interamericano de protección de los derechos humanos*. (S. Talleres Editoriales Cometa, Ed.) Madrid: Editorial Reus, S. A.

UNIÓN EUROPEA (24 de octubre de 1995). *Euro-lex*. Recuperado el 2 de febrero de 2014, de eur-lex.europa.eu: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046: es: HTML

VIASADEBA, S. (3000 a de C.). *Curso de la Máxima Auto-Realización*. Recuperado el 16 de enero de 2015, de www.spiritual-revolutionary.com: http://www.spiritual-revolutionary.com/Espanol/BG_espanol/Capitulo14/Capitulo14.htm

WIKILEAKS (2007). *www.wikileaks.org*. Recuperado el 1 de 5 de 2015, de WikiLeaks: https://www.wikileaks.org/wiki/Wikileaks/es

XATAKA (27 de 3 de 2015). *www.xataka.com*. Recuperado el 1 de 5 de 2015, de Xataka: http://www.xataka.com/otros/aprobada-la-ley-mordaza-y-la-reforma-del-codigo-penal-como-te-afecta-y-como-afecta-a-internet

JURISPRUDENCIA INTERNACIONAL

Sentencia de 27 de febrero de 2008, Estado de Renania del Norte Westfalia.

Sentencia de la Gran Sala Tribunal 7 de octubre de 2015.

Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000.

JURISPRUDENCIA NACIONAL

Sentencia T-414 de 1992, M. P. Ciro Angarita Barón. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

Sentencia T-022 de 1993, M. P. Ciro Angarita Barón. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1993/t-022-93.htm

Sentencia T-530 de 1992, M. P. Eduardo Cifuentes Muñoz. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1992/T-530-92.htm

Sentencia T-229 de 1994, M. P. Alejandro Martínez Caballero. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1994/T-229-94.htm

Sentencia T-580 de 1995, M. P. Eduardo Cifuentes Muñoz. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1995/T-580-95.htm

Sentencia SU-082 de 1995, M. P. Jorge Arango Mejía. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1995/su082-95.htm

Sentencia T-094 de 1995, M. P. José Gregorio Hernández Galindo. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1995/T-094-95.htm

Sentencia T-097 de 1995, M. P. José Gregorio Hernández Galindo. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1995/T-097-95.htm

Sentencia SU-089 de 1995, M. P. Jorge Arango Mejía. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1995/SU089-95.htm

Sentencia T-176 de 1995, M. P. Eduardo Cifuentes Muñoz. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1995/T-176-95.htm

Sentencia T-557 de 1997, M. P. Hernando Herrera Vergara. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1997/T-557-97.htm

Sentencia T-552 de 1997, M. P. Vladimiro Naranjo Mesa. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1997/t-552-97.htm

Sentencia T-462 de 1997, M. P. Vladimiro Naranjo Mesa. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1997/T-462-97.htm

Sentencia T-307 de 1999, M. P. Eduardo Cifuentes Muñoz. Recuperado en http://www.corteconstitucional.gov.co/relatoria/1999/T-307-99.htm

Sentencia T-527 de 2000, M. P. Fabio Morón Díaz. Recuperado en http://corteconstitucional.gov.co/relatoria/2000/T-527-00.htm

Sentencia T-578 de 2001, M. P. Rodrigo Escobar Gil. Recuperado en http://corteconstitucional.gov.co/relatoria/2001/T-578-01.htm

Sentencia T-1085 de 2001, M. P. Eduardo Montealegre Lynett. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2001/T-1085-01.htm

Sentencia C-646 de 2001, M. P. Manuel José Cepeda Espinosa. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2001/C-646-01.htm

Sentencia T-881 de 2002, M. P. Eduardo Montealegre Lynett. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2002/T-881-02.htm

Sentencia T-729 de 2002, M. P. Eduardo Montealegre Lynett. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

Sentencia C-1066 de 2002, M. P. Jaime Araújo Rentería. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2002/c-1066-02.htm

Sentencia C-373 de 2002, M. P. Jaime Córdoba Triviño. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2002/c-373-02.htm

Sentencia T-592 de 2003, M. P. Álvaro Tafur Galvis. Recuperado en http://corteconstitucional.gov.co/relatoria/2003/T-592-03.htm

Sentencia C-185 de 2003, M. P. Eduardo Montealegre Lynett. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2003/C-185-03.htm

Sentencia C-652 de 2003, M. P. Marco Gerardo Monroy Cabra. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2003/c-652-03.htm

Sentencia T-437 de 2004, M. P. Clara Inés Vargas Hernández. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2004/T-437-04.htm

Sentencia T-657 de 2005, M. P. Clara Inés Vargas Hernández. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2005/T-657-05.htm

Sentencia T-718 de 2005, M. P. Marco Gerardo Monroy Cabra. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2005/T-718-05.htm

Sentencia T-798 de 2007, M. P. Jaime Córdoba Triviño. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2007/T-798-07.htm

Sentencia C-1011 de 2008, M. P. Jaime Córdoba Triviño. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm

Sentencia C-640 de 2010, Magistrado Ponente Mauricio González Cuervo. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2010/C-640-10.htm

Sentencia C-748 de 2011, Magistrado. Ponente: Jorge Ignacio Pretelt Chaljub. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

Sentencia T-855 de 2011, M. P. Nilson Pinilla Pinilla. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2011/t-855-11.htm

Sentencia SU-458 de 2012, M. P. Adriana María Guillén Arango. Recuperado en http://www.corteconstitucional.gov.co/RELATORIA/2012/SU458-12.htm

Sentencia C-317 de 2012, M. P. María Victoria Calle Correa. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2012/C-317-12.htm

Sentencia C-1016 de 2012, M. P. Jorge Iván Palacio Palacio. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2012/C-1016-12.htm

Sentencia T-144 de 2013, M. P. María Victoria Calle Correa. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2013/T-144-13.htm

Sentencia T-926 de 2013, M. P. Mauricio González Cuervo. Recuperado en http://corteconstitucional.gov.co/relatoria/2013/T-926-13.htm

Sentencia T-176A de 2014, M. P. Jorge Ignacio Pretelt Chaljub. Recuperado en http://www.corteconstitucional.gov.co/RELATORIA/2014/T-176A-14.htm

Sentencia T-277 de 2015, M. P. María Victoria Calle Correa. Recuperado en http://www.corteconstitucional.gov.co/relatoria/2015/t-277-15.htm

9. SIGLAS

ADN	Ácido Desoxirribonucleico.
AENOR	Asociación Española de Normalización y Certificación.
AEPD	Agencia Española de Protección de Datos.
AGPD	Agencia Española de Protección de Datos.
AUMF	Autorización para el Uso de la Fuerza Militar contra Terroristas.
BSI	British Standard Institution.
C.P. De C	Constitución Política De Colombia.
CC	Código Civil.
CCSC	(en inglés, Commercial Computer Security Centre), Comercial Centro de Seguridad Informática.
CE	Parlamento Europeo y del Consejo.
CERT	(Computer Emergency Response Team).
CIA	(en inglés, Central Intelligence Agency), Agencia Central de Inteligencia.
CICTE	Comité Interamericano contra el Terrorismo.
CISO	(en inglés, chief information security officer), Oficial de Seguridad de la Información o Director de Seguridad de la Información.
CJI	Comité Jurídico Interamericano.
CN	Comisiones nacionales.
COBIT	(en inglés, Control Objectives for Information Systems and related Technology), Objetivos de Control para Tecnología de Información y Tecnologías relacionadas.
CONPES	Consejo Nacional de Política Económica y Social.
CP	Código Penal.
CPACA	Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
CSIRT	(Computer Security Incident Response Team)
CURP	Clave Única de Registro de Población.
D.F.	Distrito Federal.

DADH	Convención Americana sobre Derechos Humanos.
DIAN	Dirección de Impuestos y Aduanas Nacionales.
DRAE	Diccionario de Lengua Española (Real Academia Española, Diccionario de La Lengua Española.
DTI	(en inglés, Department of Trade and Industry), Departamento de Comercio e Industria.
DUDH	Declaración Universal de los Derechos Humanos.
E.P. L	Ejército Popular de Liberación.
EC	Evaluación de la Conformidad.
EMA	Entidad Mexicana de Acreditación.
ESE	Empresa Social del Estado.
FONDONORMA ISO:IEC	Asociación Civil sin fines de lucro con personalidad jurídica y patrimonio propio.
Global STD	(en inglés, Global Food Safety Initiative), Iniciativa Global de Seguridad Alimentaria.
GTC	ISO:IEC Guía Técnica Colombiana.
ICONTEC	Instituto Colombiano de Normas Técnicas y Certificación.
ID	Identificación.
IDS	IPS (en inglés, Intrusion Detection System), Sistema de Detección de Intrusiones.
IEC	(en inglés, International Electrotechnical Commission), Comisión Electrotécnica. Internacional.
IFAI	Instituto Federal de Acceso a la Información Pública.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
INCODER	Instituto Colombiano de Desarrollo Rural.
IP	Protocolo de Internet.
IRAM-ISO-IEC	Instituto Argentino de Normalización y Certificación.
ISACA	(Information Systems Audit and Control Association).
ISO	(en inglés, International Organization For Standardization), Organización Internacional de Normalización.
ITGI	(Governance Institute).
ITIL	(en inglés, Information Technology Infrastructure Library), Servicios de Tecnologías de la Información.
LEPD	Ley Estatutaria De Protección De Datos.

LOPD	Ley Orgánica de Protección de Datos.
NCC	(National Computing Centre).
NCh-ISO-IEC	Norma Chilena de Gestión de Calidad.
NFPA	Asociación Nacional de Protección contra Incendios de los Estados Unidos.
NICSP	Normas Internacionales de Contabilidad para el Sector Público.
NIIF	Normas Internacionales de Información Financiera.
NIST	(en inglés, National Institute of Standards and Technology), Instituto Nacional de Normas y Tecnología.
NMX	Normas Mexicanas.
NTC	Instituto Colombiano de Normas Técnicas y Certificación.
NTC-ISO-IEC	Norma Técnica Colombiana.
OCDE	Organización para la Cooperación y el Desarrollo Económico.
OEA	Organización de los Estados Americanos.
OIT	Organización Internacional del Trabajo.
ONAC	Organismo Nacional de Acreditación.
ONUDI	Organización de las Naciones Unidas para el Desarrollo Industrial.
OTAN	Organización del Tratado del Atlántico Norte.
P.T. R.	Partido Revolucionario de los Trabajadores.
PC	Principio Superior Constitucional de Dignidad.
PCI DS	(en inglés, Payment Card Industry Data Security Standard), Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.
PCI SSC	Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago.
PD	Protección de Datos.
PHVA	(planear, hacer, verificar y actuar).
PILA	Planilla Integrada de Liquidación de Aportes.
PJ	Principios jurisprudenciales.
PL	Principios Legales.
PNR	(en inglés, Passenger Name Record), Registro de Nombres de los Pasajeros.

PQR	(en inglés, Procedure Qualification Record), Registro de la Calificación del Procedimiento.
PTI	Política de Tratamiento de la Información.
RAUCS	(Recolectarlo, Almacenarlo, Usarlo, Circularlo o Suprimirlo).
RFC	Registro Federal de Contribuyentes.
RFID	(en inglés, Radio Frequency Identification), Identificación por Radio Frecuencia.
RNBD	Registro Nacional de Bases de Datos.
RUP	Registro Único de Proponentes.
SGSI	Sistema de Gestión de la Seguridad de la Información.
SI	Seguridad de la Información.
SIC	Superintendencia de Industria y Comercio.
SIEM	(en inglés Security Information and Event Management) Gestión de eventos y de la seguridad de la información.
SMLMV	Salario mínimo legal mensual vigente.
SMS	Secretaría de Seguridad Multidimensional.
TCI	Tecnologías de la información y la comunicación.
TCP:IP:	(en inglés Transmission Control Protocol), Protocolo de Control de Transmisión, Protocoló de Internet.
TCSEC	(en inglés, Trusted Computer System Evaluation Criteria) Criterios de Evaluación del Sistema Informático de Confianza.
UE	Unión Europea.
UNIT-ISO:IEC	Instituto Uruguayo de Normas Técnicas.
UPAC	Unidades de Poder Adquisitivo Constante.
USA	(en inglés, United States Of America), Estados Unidos de América.
USD	(en inglés, United State's Dollar) Dólares Estadounidenses.
v. gr.	Verbi Gracia.
VIH	Virus de la Inmunodeficiencia Humana.
VPN	(en inglés, Virtual Private Network), Red Privada Virtual.