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

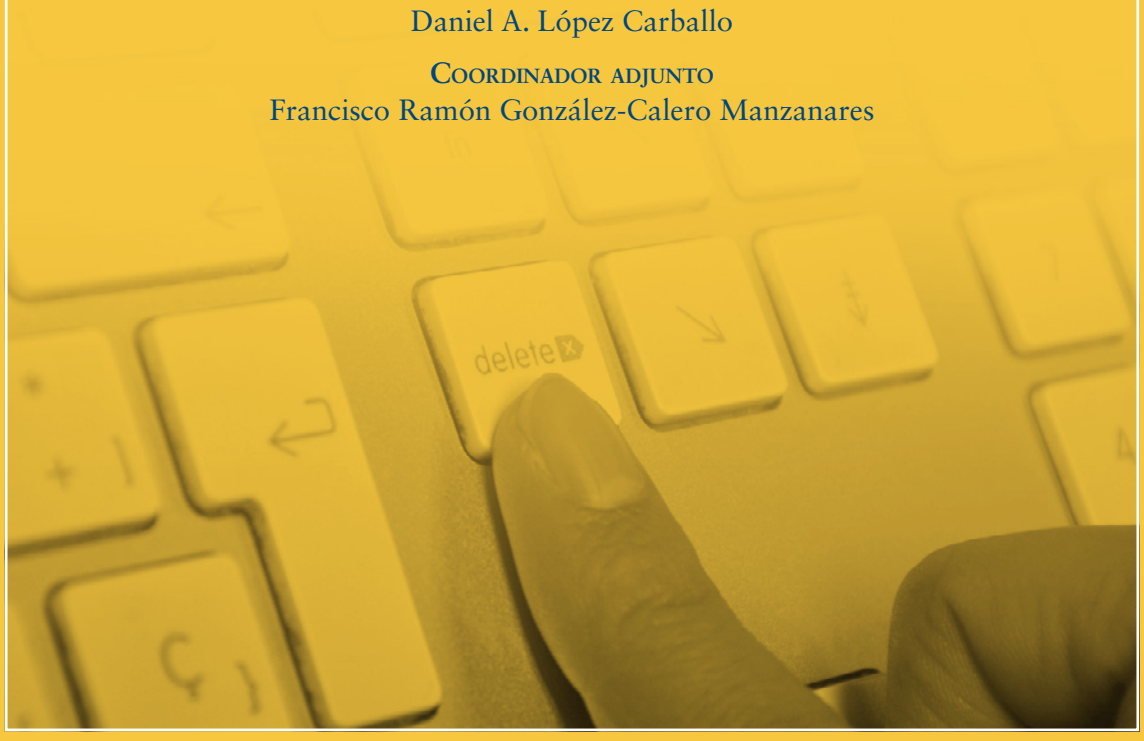
ACCÉSIT 2014

Protección de datos y *habeas data:* una visión desde Iberoamérica

Autores del estudio
Aristeo García González · Claudio Ragni Vargas · Cláudio Roberto Santos
Cynthia Téllez Gutiérrez · Daniel A. López Carballo · Dulcemaría Martínez Ruiz
Édgar David Oliva Terán · Francisco Ramón González-Calero Manzanares
Héctor E. Guzmán Rodríguez · Javier Villegas Flores · João Ferreira Pinto
Jorge Augusto Tena Ramírez · Jorge Luis García Obregón · José Luis Colom Planas
Laura Vivet Tañà · Marta Sánchez Valdeón · Matilde Susana Martínez
Romina Florencia Cabrera · Ruth Benito Martín
Salvador Serrano Fernández · Wilson Rafael Ríos Ruiz

Coordinador del estudio
Daniel A. López Carballo

Coordinador adjunto
Francisco Ramón González-Calero Manzanares



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

PROTECCIÓN DE DATOS Y *HABEAS DATA:* UNA VISIÓN DESDE IBEROAMÉRICA

PROTECCIÓN DE DATOS Y *HABEAS DATA:* UNA VISIÓN DESDE IBEROAMÉRICA

Autores del estudio

Aristeo García González · Claudio Ragni Vargas · Cláudio Roberto Santos · Cynthia Téllez Gutiérrez
Daniel A. López Carballo · Dulcemaría Martínez Ruiz · Édgar David Oliva Terán
Francisco Ramón González-Calero Manzanares · Héctor E. Guzmán Rodríguez · Javier Villegas Flores
João Ferreira Pinto · Jorge Augusto Tena Ramírez · Jorge Luis García Obregón · José Luis Colom Planas
Laura Vivet Tañà · Marta Sánchez Valdeón · Matilde Susana Martínez · Romina Florencia Cabrera
Ruth Benito Martín · Salvador Serrano Fernández · Wilson Rafael Ríos Ruiz

Coordinador del estudio

Daniel A. López Carballo

Coordinador adjunto

Francisco Ramón González-Calero Manzanares

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

Agencia Española de Protección de Datos

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

Convención Interamericana de Derechos Humanos

Artículo 11: Protección de la honra y de la dignidad.

1. *Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.*
2. *Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.*
3. *Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.*

El presente Estudio fue premiado con el Accésit en la XVIII Edición de los Premios de Investigación de la Agencia Española de Protección de Datos, en la categoría de Protección de Datos en Países Iberoamericanos.

Madrid, 28 de enero de 2015,
Día Internacional de la Protección de Datos.

ÍNDICE

PRÓLOGO 8

PRESENTACIÓN DEL ESTUDIO 10

1. PUNTO DE PARTIDA 12

2. PAÍSES CON LEGISLACIÓN ESPECÍFICA EN MATERIA DE PROTECCIÓN DE DATOS ... 19

2.1 ANDORRA 19
2.2 ARGENTINA 25
2.3 CHILE 32
2.4 COLOMBIA 38
2.5 COSTA RICA 52
2.6 ESPAÑA 59
2.7 MÉXICO 79
2.8 NICARAGUA 91
2.9 PERÚ 94
2.10 PORTUGAL 102
2.11 REPÚBLICA DOMINICANA 107
2.12 URUGUAY 122

3. PAÍSES CON LEGISLACIÓN EN MATERIA DE PRIVACIDAD 127

3.1 PARAGUAY 127
3.2 PUERTO RICO 130

4. PAÍSES CON LEGISLACIÓN EN MATERIA DE *HABEAS DATA* 133

4.1 BOLIVIA 133
4.2 BRASIL 136
4.3 ECUADOR 141
4.4 GUATEMALA 145
4.5 HONDURAS 147
4.6 PANAMÁ 152

5. OTROS PAÍSES Y EL TRATAMIENTO DE LA PROTECCIÓN DE LOS DATOS PERSONALES 156

5.1 CUBA 156
5.2 EL SALVADOR 157
5.3 VENEZUELA 159

6. EQUILIBRIO ENTRE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS ... 162

7. TRANSFERENCIAS INTERNACIONALES DE DATOS 166

8. RELACIONES CON CANADÁ Y ESTADOS UNIDOS 178

8.1 CANADÁ 178
8.2 ESTADOS UNIDOS 179

9. RELACIONES CON LA UNIÓN EUROPEA 184

10. CONCLUSIONES 199

TABLAS Y ANEXOS 202

— CONSTITUCIONES NACIONALES 202
— LEGISLACIONES NACIONALES PROTECCIÓN DE DATOS 206
— LEGISLACIÓN ESPECIFICA COMPARADA 208
— NIVELES DE PROTECCIÓN CONFORME A LA NORMATIVA PROPIA DE CADA PAÍS 209
— PAÍSES CON NIVEL ADECUADO DE PROTECCIÓN 210
— PAÍSES ESPECIALMENTE RELACIONADOS 210
— PROYECTOS LEGISLATIVOS EN TRÁMITE 210
— TENTATIVAS LEGISLATIVAS FALLIDAS 210
— ORGANISMOS Y AUTORIDADES DE CONTROL 211
— SUPUESTOS O CONDICIONES PARA REALIZAR TRANSFERENCIAS INTERNACIONALES DE DATOS 212

BIBLIOGRAFÍA 214

— OBRAS CONSULTADAS 214
— PÁGINAS WEB DE REFERENCIA CONSULTADAS 215

ÍNDICE DE AUTORES 217

PRÓLOGO

Los Premios de Investigación sobre el derecho a la protección de datos en países iberoamericanos que convoca anualmente la Agencia Española de Protección de Datos tienen por objeto fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos en materia de protección de datos de carácter personal. Esta obra, *Protección de datos y habeas data: una visión desde Iberoamérica,* ha sido galardonada con el accésit de la XVIII edición por recoger en una investigación práctica y comparada la legislación específica sobre protección de datos de diferentes naciones.

Este libro es el resultado de un esfuerzo colectivo impulsado por 21 especialistas de distintos países iberoamericanos, cuya justificación descansa, en palabras de sus autores, en "la necesidad de contar con una panorámica sobre las diferentes normativas en Iberoamérica que facilite a los actores políticos, económicos y sociales la toma de decisiones que puedan afectar a la protección de datos de carácter personal".

En los últimos quince años, un número significativo de países de la región han ido incorporando no sólo una legislación específica en materia de protección de datos personales sino también, y quizás sea este uno de los aspectos más relevantes, un conjunto de instrumentos organizativos y legales para asegurar unas garantías adecuadas y suficientes y, en consecuencia, una protección efectiva para los ciudadanos.

Argentina, Chile, Colombia, Costa Rica, México, Nicaragua, Perú y Uruguay cuentan con una ley propia en este sentido. Ello ha significado que, en la actualidad, más de 150 millones de ciudadanos iberoamericanos disponen, junto al tradicional amparo del *habeas data*, de normas que permiten controlar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar dichas garantías. Sin embargo, y aun reconociendo la gran labor desarrollada en un período tan corto, es evidente que aún queda mucho por hacer y que será necesario diseñar estrategias adaptadas a las necesidades y peculiaridades de aquellos países que aún no cuentan con un marco normativo propio en la materia.

Con este objetivo, trabajos como el reconocido con el accésit van a ser de gran utilidad para otros investigadores en la medida en que contribuyen a mostrar una imagen de la rica y variada realidad legislativa en Iberoamérica, sin desconocer la existencia de elementos comunes como una realidad jurídica basada en la transparencia y el acceso a la información, o la generalización del instituto del *habeas data*, además de la influencia que ha tenido en esta evolución la normativa europea y, en particular, la española.

Por ello, resulta primordial seguir avanzando en la búsqueda de puntos de encuentro y de elementos integradores que favorezcan la deseable aproximación entre las legislaciones. En este afán armonizador, merece un apartado especial la labor que viene desarrollando la Red Iberoamericana de Protección de Datos como foro de encuentro e intercambio de información "para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este

derecho", según se recoge en su reglamento interno. O iniciativas como la que está impulsando en la actualidad la Organización de Estados Americanos, con la colaboración activa de la Red Iberoamericana, para tratar de dotar a la región de una Ley Modelo en la materia.

La obra se sitúa, en este contexto, como un intento loable de sus autores por acercar conceptos y categorías jurídicas entre las legislaciones nacionales, continuando así la senda iniciada en la edición anterior del Premio, en la que se reconoció el trabajo de un glosario de términos y usos lingüísticos.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos

PRESENTACIÓN DEL ESTUDIO

El derecho de las personas sobre la protección de sus datos, íntimamente ligado al ámbito del derecho a la imagen y al honor, se encuentra regulado en la mayor parte de las legislaciones iberoamericanas a través del denominado *habeas data,* en calidad de garantía constitucional. A mayor abundamiento, cada vez son más los Estados que cuentan con normas específicas en materia de protección de datos, adaptando el resto de leyes, decretos y otra normativa para una mejor salvaguarda de lo derechos de las personas, así como su tutela judicial efectiva.

En mundo globalizado, en el que la movilidad, no sólo geográfica, si no también económica, profesional, bancaria, juega un papel tan importante, las transferencias internacionales de datos, son una realidad cada vez más frecuente debido a la globalización y geodeslocalización de Internet y las nuevas tecnologías como el *Cloud Computing.* En el ámbito económico, aspectos como la compraventa de inmuebles, la implantación de las empresas en diferentes países, así como la propia movilidad de las personas, implican un flujo constante de información, que ha de someterse a los cánones internacionales y la legislación propia de cada Estado, en aras de proteger la intimidad de las personas, garantizando su privacidad y la protección de su información de carácter personal.

La protección de la privacidad es un derecho fundamental reconocido por las Naciones Unidas que protege la libertad individual, la libertad de expresión, la intimidad y la dignidad personal. Este derecho contiene dentro de sí la protección de datos y la figura del *Habeas Data,* según afirma la propia Organización de Estados Americanos. El Consejo de Europa lo define como un derecho humano fundamental. Por su parte la Declaración Universal de Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos definen a la privacidad como un derecho: «nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación».

La garantía constitucional del *habeas data* impone ciertas obligaciones a las entidades, públicas y privadas, que tratan la información. Los datos recogidos deberán ser utilizados para los fines específicos y explícitos para los que fueron recabados, debiéndose garantizar la seguridad de los mismos y controlando el acceso por parte de personas no autorizadas.

Los ciudadanos tienen derecho a conocer la legalidad en la recopilación de sus datos, quedando estos habilitados para que, en caso de haberse recabado de forma ilegal, puedan solicitar la correspondiente sanción a los responsables. Esta acción constitucional aumenta el nivel de transparencia en el acceso a la información, así como el tratamiento y personas o entidades que acceden o son cesionarios de la misma.

Cada vez son más los países iberoamericanos que cuentan con una legislación específica en materia de protección de datos, así como de medios legales y organizativos para proteger el derecho a la privacidad y al honor de los ciudadanos. Argentina cuenta en su acervo normativo con la Ley 25.326 de Protección de Datos del 2 noviembre de 2000, Colombia aprobaba la Ley Estatutaria 1581 por la cual se dictan disposiciones generales para la protección de datos personales, Perú cuenta con la Ley 29733 de Protección de Datos Personales y Uruguay desde 2008 con la Ley 18.331 de Protección de Datos Personales y Acción *Habeas Data,* entre otras normas y países. Actualmente Honduras, Chile, México se encuentran desarrollando nuevas normas o actualizando sus normas y otros países como Ecuador han anunciado próximos desarrollos normativos.

En este contexto nace el presente Estudio, como análisis de los diferentes países, sus normas y jurisprudencia, clasificándolos en cuatro bloques temáticos: países con legislación específica

en materia de protección de datos, países con legislación en materia de privacidad, países con legislación en materia de *habeas data* y otros países y el tratamiento de la protección de los datos personales. Dentro de los países del primer grupo se analizan aspectos fundamentales como bien jurídico protegido, calidad de los datos, autoridades de control, información y consentimiento o medidas de seguridad.

Por su especial interés y actualidad se trata en tema aparte el equilibrio entre acceso a la información o transparencia y protección de datos. El documento se completa con un capítulo dedicado a las especiales relaciones existentes entre Iberoamérica con Estados Unidos y Canadá, y otro dedicado a la Unión Europea, en la que se ha tratado la Propuesta de Reglamento General de Protección de Datos, actualmente en proceso legislativo destacando las nuevas figuras, tendencias y herramientas para una mejor protección de este derecho fundamental, no debemos olvidar que en juego puede estar conseguir o perder, el reconocimiento de un nivel adecuado de protección. Debido a su importancia, se ha creado un capítulo destinado a las transferencias internacionales de datos y los requisitos que establecen los diferentes países para su validez.

Para finalizar se han incluido diversas tablas y anexos comparativos entre las diferentes normativas, proyectos legislativos en trámite y aquellos que han quedado en meras tentativas, así como una tabla recogiendo el tratamiento de las transferencias internacionales de datos y los requisitos que establecen los diferentes países.

Es por ello que la utilidad de este Estudio, su valor, su justificación y la necesidad de llevarlo a cabo nace de la necesidad de contar con una panorámica sobre las diferentes normativas en Iberoamérica que facilite a los actores políticos, económicos y sociales la toma de decisiones que puedan afectar a la protección de datos de carácter personal.

Iberoamérica avanza en la legislación de un derecho fundamental inherente a las personas, tanto mediante una regulación específica como dentro de la figura de la garantía constitucional del *Habeas Data,* hacia un marco jurídico común que cree un espacio de seguridad jurídica tanto en el ámbito empresarial y las transacciones económicas y de servicios, como de la libre circulación de las personas y sus relaciones más allá de su espacio cotidiano, donde Internet y las nuevas tecnologías juegan un papel fundamental y los datos se propagan a gran velocidad y en gran volumen.

Daniel A. López Carballo
Coordinador del estudio

1. PUNTO DE PARTIDA

Se han hecho numerosas conceptualizaciones sobre *habeas data,* pero de una manera sencilla y clara, podemos decir que se refiere a un tipo de acción constitucional de libre ejercicio para cualquier ciudadano que considere que sus datos personales están siendo manipulados indebidamente y sin su autorización en una base de datos o registro informático, por parte de una persona natural o jurídica. Su finalidad es pedir la eliminación y/o corrección de la información.

Al hacer un análisis del *habeas data* y su justificación regulatoria, es imperante saber la evolución de esta figura. El *habeas data,* no es un tema reciente, ni autóctono de Latinoamérica, sino que al contrario, tiene mucho tiempo de venir evolucionando y adaptándose a las necesidades sociales, económicas y tecnológicas de la humanidad y tiene sus orígenes en el viejo continente.

Podríamos ubicar el nacimiento del *habeas data* en su pariente cercano, el *habeas corpus*[1]. El cual data desde lo tiempos de «Juan sin Tierra[2]» en la vieja Inglaterra, donde existe registro histórico de la primera manifestación o aplicación de una medida de protección al derecho a la intimidad, pero en este caso se protegía al *habeas corpus,* entendiéndose la traducción en latín como «traer el cuerpo», el caso concreto se daba en injustos encarcelamientos donde se compelía a presentar el cuerpo, la persona en físico que se pretendía investigar su encarcelamiento.

Con el desarrollo de las tecnologías de las telecomunicaciones: la recolección, clasificación y conservación de la información surgió de la mano con los gigantescos ordenadores que ocuparon espacios inmensos en las universidades más prestigiosas del mundo.

Así, como las redes de comunicaciones —en un inicio internas— que luego tomaron importantes dimensiones, tanto en los ámbitos económicos, sociales y tecnológicos. Podemos decir, que hoy en día existen cantidades de información —casi infinitas— que circulan y se agregan a estas redes de comunicaciones, teniendo como consecuencia un flujo de información de los individuos, ignorado por sus titulares. Esta necesidad social, económica y tecnológica llevo a esgrimir aforismos latinos como el *status positivos socialis* (que encuadra las relaciones jurídicas propias de los derechos económicos y sociales), el *status activus processualis* (que abarca los distintos mecanismos de garantía jurisdiccional de los derechos fundamentales) y un status de *habeas data* (que integra los mecanismos de protección de la información personal).

Como parte del concepto de vida privada, es reconocido internacionalmente el derecho a la intimidad personal y familiar, el derecho a la imagen propia y el derecho al secreto de las comunicaciones, como derechos inalienables, conforman el fuero interno de la persona. Es por

---

1 Institución jurídica que se ejercita a través de una acción constitucional que persigue evitar arrestos y detenciones arbitrarias, asegurando los derechos básicos de la víctima; estar vivo y consciente, ser escuchado por la justicia y poder saber de qué se le acusa. En todas las legislaciones se presentan garantías mínimas para el detenido como son ser presentado en un plazo preventivo determinado ante un juez, quien tiene facultad para ordenar libertad inmediata del detenido si no se encontrara motivo suficiente de arresto.

2 Juan I de Inglaterra más conocido como Juan sin Tierra (originalmente Sans-Terre en francés, Lacklanden inglés), fue rey de Inglaterra y señor de Irlanda. Reinó en Inglaterra desde el 6 de abril de 1199 hasta su muerte en 1216. Sucesor del trono de su hermano mayor, Ricardo I de Inglaterra (conocido como «Ricardo Corazón de León»). Juan se ganó el apodo de «Sin Tierra» debido a su carencia de herencia por ser el menor de los hijos y por su pérdida de los territorios en Francia; también fue apodado «Espada Suave» por su conocida ineptitud militar. Fue un rey Plantagenet o de la línea angevina.

ello que el *habeas data* —que significa «traer los datos»— tiene como fin primario evitar ciertos excesos del poder informático.

En Alemania, con la promulgación de la «Hessiches Datenschutzgesetz[3]» en 1970, por parte del Parlamento de Estado alemán de Hesse, este territorio se convirtió en el primero en el mundo con una norma dirigida a la protección de datos, su fin es impedir la lesión a los derechos relacionados con los datos personales de los individuos, se pautan normas respecto al almacenamiento, transmisión, modificación o cancelación de los datos personales en base de datos. En el 1977, el Parlamento Federal Alemán adopta a nivel nacional la normativa y aprueba la Bundesdatenschutzgesetz[4]. Creando así un Bundersbeauftrager furden datenshutz[5].

En Suecia, en el 1973, se promulgó el *Data lag*[6]. Por medio de esta normativa se crea un registro público específico, que ordena registrar los ficheros electrónicos de datos de carácter público o privado. También se autoriza a que este registro extienda licencias para el manejo de datos personales y se nombró un ente regulador e inspeccionador de datos personales.

En Estados Unidos de América, en 1974, en medio del escándalo Watergate y ante el temor sobre el uso que el Gobierno pudiera hacer de los ordenadores y de los sistemas informáticos, el Congreso norteamericano promulga el *Privacy Act*[7].

En Portugal en 1976 se estableció en la Constitución el artículo 35 en la materia de protección de datos que reza: «Todos los ciudadanos tienen derecho a tomar conocimiento de los datos contenidos en ficheros o registros informáticos a su respecto, pudiendo exigir su rectificación y actualización, sin perjuicio de lo dispuesto por las leyes sobre secretos de Estado (...). Está prohibido el acceso a ficheros y registros informáticos para conocer datos personales de terceros, o por interconexión, salvo los casos excepcionales previstos por la Ley, la informática no puede ser para el tratamiento de datos referidos a convicciones filosóficas o políticas, de filiación partidaria o sindical, fe estadísticos, que no se identifiquen individualmente».

En 1978, Francia estableció la Commission Nationale de la Informatique et des Libertes[8].

---

3 Se puede traducir como la Ley de Protección de Datos de Hesse, Ley de Privacidad de la administración pública del Estado de Hesse, Alemania. Entró en vigor en 1970 y es el primer y más antiguo formal de la ley de protección de datos en el mundo.

4 La Ley Federal de Protección de Datos (BDSG) gobierna junto con las leyes de protección de datos en Alemania y otras regulaciones sectoriales que se ocupan de los datos personales, en los sistemas de información y comunicación son procesados o manualmente. Se establece la Directiva de protección de datos.

5 Comisario Federal para la Protección de Datos.

6 Significa; los datos fueron.

7 La Ley de Privacidad de 1974, Ley Federal de los Estados Unidos, que establece un Código de Feria Información Práctica que rige la recopilación, mantenimiento, uso y difusión de la información de identificación personal sobre los individuos que se mantiene en los sistemas de registros por las agencias federales. Un sistema de registros es un grupo de registros bajo el control de un organismo a partir del cual la información es recuperada por el nombre de la persona o por algún identificador asignado al individuo. La Ley de Privacidad requiere que las agencias dan el aviso público de sus sistemas de registros mediante la publicación en el Registro Federal. La Ley de Privacidad prohíbe la revelación de información de un sistema de registros salvo con el consentimiento escrito de la persona sujeta, a menos que la divulgación es en virtud de una de las doce excepciones legales. La ley también proporciona a los individuos con un medio por el cual pueda gestionar su acceso a una modificación de sus registros, y establece varios requisitos de mantenimiento de registros de la agencia.

8 La Comisión Nacional de la Informática y las Libertades es responsable de asegurar que la tecnología de la información está al servicio de los ciudadanos y que no afecta a la identidad humana, o los derechos del hombre, o la privacidad, o individuo y las libertades públicas.

En 1978, En España al igual que Portugal, se incorpora a la Constitución el inciso 4 del artículo 18, que dice: «La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos...».

En 1981 el Consejo de Europa aprueba el Convenio N.º 108, de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter persona, con el fin «es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")».

En 1984, el Parlamento británico promulgó el Data *Protection Act*[9]. En ese mismo año, la Constitución brasileña, en su artículo 5, inc. 72, expresa que se concederá el *habeas data* para: a) asegurar el conocimiento de información relativa a la persona del demandante, que consiste en registros o bancos de datos de entidades gubernamentales o de carácter público y b) rectificar datos cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo. En este país se tramita el *habeas data* como un procedimiento distinto al del recurso de amparo.

En 1995 se aprueba en la Unión Europea la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[10], con el objeto de obligar a los Estados Miembros a garantizar «la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales».

En el año 2000 la Unión Europea da un paso más al incluir en la Carta de los Derechos Fundamentales de la Unión Europea[11] el derecho a la protección de datos de carácter personal en su artículo 8.º «1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».

Y al consagrar en su artículo 7 que: «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones», lo que da lugar a que se establezca una especial regulación para las comunicaciones electrónicas a través de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de

---

9 La Ley de Protección de Datos de 1998 (DPA) es una ley del Parlamento del Reino Unido de Gran Bretaña e Irlanda del Norte que define la legislación británica sobre el tratamiento de datos sobre personas vivas identificables. Es la pieza principal de la legislación que rige la protección de los datos personales en el Reino Unido. Aunque la propia Ley no menciona la privacidad, que se promulgó para que la legislación británica en línea con la Directiva de la UE sobre protección de datos de 1995 que obligaba a los Estados miembros para proteger los derechos y libertades fundamentales de las personas y, en particular, su derecho a la privacidad con respecto al tratamiento de datos personales. En la práctica, ofrece una manera para que las personas para controlar la información sobre sí mismos. La mayor parte de la Ley no se aplica al uso doméstico, por ejemplo, mantener una libreta de direcciones personal. Cualquiera que tenga datos personales para otros fines está legalmente obligado a cumplir con esta Ley, sin perjuicio de algunas excepciones.

10 Diario Oficial de las Comunidades Europeas n.º L 281 de 23/11/1995.

11 Diario Oficial de las Comunidades Europeas n.º C 364/1 de 18.12.2000.

los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[12].

Es por ello, y con el fin de garantizar la protección de los principios que inspiran el *habeas data,* que las diferentes Constituciones nacionales en la región contemplan esta figura como veremos a continuación. Se hace por ello palpable que es digno de protección constitucional un uso leal, adecuado, pertinente y no excesivo de los diversos tratamientos de datos. De igual forma se constata que ese uso leal sólo puede alcanzarse mediante principios de transparencia en la información, obtención de consentimientos, creación de procedimientos de Tutela de Derechos e implantación de medidas y salvaguardar tendentes a garantizar el deber de secreto y seguridad de la información.

La Constitución peruana en 1993 prohíbe en el articulo 2, inciso 6, que los servicios informáticos, computarizados o no, públicos o privados, suministren informaciones que afecten la intimidad personal o familiar. En el art. 200 del mismo cuerpo de leyes se establece el procedimiento del *habeas data*.

En Argentina, con la Constitución Federal de 1994, el artículo 43 dice: «(...) Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad que conste en registros o bancos de datos públicos destinados a proveer informes, y en caso de falsedad y discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto a las fuentes de información periodísticas. (...)»

La Constitución del Honduras, recoge el derecho al honor, a intimidad personal, familiar y la propia imagen, desarrollando en su artículo 182 el derecho fundamental de acceso a la información pública y privada, así como la garantía constitucional de *habeas data:* «El Estado reconoce la garantía de *Habeas Corpus* o Exhibición Personal, y de *Habeas Data*. En consecuencia en el *Habeas Corpus* o Exhibición Personal, toda persona agraviada o cualquier otra en nombre de ésta tiene derecho a promoverla; y en el *Habeas Data* únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados de la manera siguiente: (…) 2. El *Habeas Data:* Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en caso de que fuere necesario, actualizarla, rectificarla y-o enmendarla. Las acciones de *Habeas Corpus* y *Habeas Data* se ejercerán sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles o inhábiles y libre de costas. Únicamente conocerá de la garantía del *Habeas Data* la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tendrá la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y la propia imagen. Los titulares de los órganos jurisdiccionales no podrán desechar la acción de *Habeas Corpus* o Exhibición Personal e igualmente tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad y a la seguridad personal. En ambos casos, los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones constitucionales, incurrirán en responsabilidad penal y administrativa. Las autoridades que ordenaren y los agentes que ejecutaren el ocultamiento del detenido o que en cualquier forma quebranten esta garantía incurrirán en el delito de detención ilegal».

La República del Ecuador en su Carta Magna de 2008, establece que «toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o

---

12 Diario Oficial de la Unión Europea núm. 201, de 31 de julio de 2002.

privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados».

Colombia recoge en el artículo 15 de su Constitución Política 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. De igual modo, 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. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución».

Nos encontramos en Iberoamérica que cada vez son más los países que siguen la tendencia de regular mediante una norma específica la protección efectiva de los datos personales y la privacidad de las personas. La aprobación en Colombia de la Ley Estatutaria 1581 por la cual se dictan disposiciones generales para la protección de datos personales, Perú aprobó la Ley 29733 de Protección de Datos Personales, junto con la y Uruguay desde 2008 con la Ley 18.331 de Protección de Datos Personales y Acción *Habeas Data,* la Ley Orgánica 172-13 de protección de datos de carácter personal de la República Dominicana, entre otras normas. Otros países como Chile, han iniciado la reforma de sus normas en materia de protección (cuya fase de consulta de pública ya ha finalizado) y un tercer bloque se encuentra en proceso de adoptar nuevas normas como son los casos de Honduras (en 2014 se conocía el anteproyecto de norma) y Ecuador (que ya en 2010 iniciaba el primer intento de tramitar Ley de Protección a la Intimidad y a los Datos Personales presentada por el Asambleísta Vethowen Chica Arévalo).

Esa necesidad de legislar por parte de los países en aras a una mayor protección de los derechos de las personas sobre sus datos, se recoge, a modo de ejemplo, en el Dictamen emitido por la Comisión de Puntos Constitucionales de la Cámara de Diputados[13] de México, donde se puso de manifestó que «… sin duda, es necesario la protección jurídica de los datos personales, ya que el tratamiento por mecanismos electrónicos y computarizados que se han incorporado de manera creciente a la vida social y comercial, ha conformado una cuantiosa red de datos que, sin alcanzar a ser protegidos por la ley, son susceptibles de ser usados de ilícita, indebida o en el mejor de los casos inconvenientemente para quienes afectan. Si a ello se le suma el importante papel que las bases de datos desempeñan en el mundo tecnificado y globalizado…».

La intensa actividad legislativa que vive Iberoamérica en materia de protección de datos se une a la acción y nacimiento de organismos de control nacionales como la Autoridad Nacional de Protección de Datos de Perú, la Agencia de Protección de Datos de los Habitantes en Costa Rica, o el fortalecimiento de otras ya existentes y de reconocida trayectoria como el Instituto Federal de Acceso a la Información y Protección de Datos en México o la Dirección Nacional de Protección de Datos y su homóloga en Buenos Aires de Argentina.

Podemos ver que la evolución del *habeas data* a nivel mundial es producto del contexto socioeconómico, que despunta en la necesidad de una acción constitucional de protección al

---

13 «Dictamen de la Comisión de Puntos Constitucionales, con proyecto de decreto que adiciona un párrafo segundo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos», publicado en la Gaceta Parlamentaria, el 11 de diciembre de 2008.

derecho de la intimidad de los individuos, donde toma total importancia este análisis realizado en una investigación académica[14] sobre la materia:

«En un Estado de Derecho, la protección de los derechos fundamentales se constituye en pilar fundamental de la democracia. El mundo de la informática introduce en la protección de tales derechos una serie de variantes que influyen de manera decisiva en el quehacer jurídico mundial. Es en este contexto en donde el derecho sustantivo y el procesal necesitan transformarse para cobijar de forma efectiva las libertades públicas relacionadas con la protección de las bases de datos o *habeas data*. La libertad de información, de expresión, de acceso a la justicia, de privacidad e intimidad se convierten en importantes derechos para revisar en la legislación y jurisprudencia nacionales (…)»

«Sin embargo, no del todo está a la deriva la salvaguarda de esta libertad informática. De la interpretación de normas constitucionales e internacionales y su respectiva concordancia, es posible esbozar un marco regulación al respecto y es mediante el recurso de amparo que el individuo o ciudadano obtiene, al menos en la teoría, una posibilidad para recurrir a los órganos que imparten justicia y obtener así respuesta cuando su derecho al acceso a las bases de datos que contienen sus calidades personales, por ejemplo, ha sido vulnerado.»

El Consejo de Europa entiende el derecho a la privacidad como un derecho humano fundamental, debe recordarse que la propia Declaración Universal de Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos establecen que «nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación», por lo que «toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques».

La propia Organización de Estados Americanos, en la Asamblea General celebrada en La Antigua (Guatemala), tomando como base la creciente importancia de la privacidad y la protección de datos personales, así como la necesidad de fomentar y proteger el flujo transfronterizo de información en las Américas; teniendo en cuenta que la privacidad y la protección de datos personales cuya divulgación podría afectar derechos legítimos de su titular, la resolución CJI/RES. 186 (LXXX-O/12), denominada «Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas», presentada por el Comité Jurídico Interamericano, así como de la sesión de la Comisión de Asuntos Jurídicos y Políticos celebrada el 13 de noviembre de 2012, con la participación del Comité Jurídico Interamericano, los Estados miembros y la Secretaría General, para analizar los estudios recibidos sobre Protección de Datos Personales y considerar la posibilidad de un marco regional en esta área y en este sentido:

«Invitar a los Estados miembros, cuando corresponda, y a la Secretaría General, a través de su Departamento de Derecho Internacional, que apoyen la labor que realiza la Red Iberoamericana de Protección de Datos Personales (RIPD) y que participen activamente en las Conferencias Mundiales de las Comisiones de Privacidad y Protección de Datos Personales.

Encomendar al Comité Jurídico Interamericano que formule propuestas a la Comisión de Asuntos Jurídicos y Políticos sobre las distintas formas de regular la protección de datos personales, incluyendo un proyecto de Ley Modelo sobre Protección de Datos Personales, tomando en cuenta los estándares internacionales alcanzados en la materia.

---

[14] Universidad de Costa Rica, Facultad de Derecho. El *Habeas Data* (2000) (Trabajo Académico). Curso de Derecho Informático DE-2108. Profesor del curso: Lic. Guillermo Augusto Pérez Merayo. Desarrollado por: Arias Kristy, Baltodano Fernando, Cavallini Angelo, Quesada Carlos, Briones Senel. Descargado el día 25 de marzo. Disponible en:
http://www.derecho.ucr.ac.cr/~gapmerayo/cursos/cursoDI/trabajosclase/habdata/habdata.htm

Encomendar a la Secretaría General que siga promoviendo canales de colaboración con otras organizaciones internacionales y regionales que realizan esfuerzos en materia de protección de datos, a fin de facilitar el intercambio de información y cooperación.

Encomendar a la Secretaría General que identifique nuevos recursos para apoyar los esfuerzos de los Estados Miembros que faciliten el acceso a la información pública y protección de datos personales, y alentar a otros donantes a que contribuyan en esta labor.»

Debe por último atenderse a las especiales relaciones que existen entre los países iberoamericanos y Estados Unidos y la Unión Europea, tanto en el plano personal de sus ciudadanos, como político, social y empresarial entre otros. La aparición de nuevos tipos delictivos y el auge de las nuevas tecnologías, el cambio de tendencia en la forma en que las personas se comunican o los flujos de datos y su tratamiento impulsan la normativación y unificación de criterios en protección de los datos. Una adecuación de los sistemas legislativos a las nuevas tendencias, en un momento en que Europa elabora un Reglamento y las personas demandan una mayor tutela y protección de su intimidad, su honor y su propia imagen.

2. PAÍSES CON LEGISLACIÓN ESPECÍFICA EN MATERIA DE PROTECCIÓN DE DATOS

2.1 ANDORRA

Constitución del Principado de Andorra

Artículo 14. Se garantiza el derecho a la intimidad, al honor y a la propia imagen. Toda persona tiene derecho a ser protegida por las leyes contra las intromisiones ilegítimas en su vida privada y familiar.

INTRODUCCIÓN A LA PECULIARIDAD DE ANDORRA

Andorra es un pequeño país situado en Europa, concretamente en los Pirineos, entre Francia y España; es de los países más pequeños del mundo por su superficie de 468 km^2 y unos 80 000 habitantes de población de los que únicamente un tercio tiene nacionalidad andorrana. A efectos de ámbito territorial, puede consultarse el art. 4 del «Reglament de la Agència Andorrana de Protecció de Dades» (RAPDA).

Desde la aprobación de la Constitución en referéndum el 14 de marzo de 1993, el sistema político de Andorra es un coprincipado parlamentario cuyos copríncipes son el Presidente de la República (Francia) y el Arzobispo de Seo de Urgell (España). No obstante, se trata de un país soberano cuyo idioma oficial es el catalán.

Dispone de Autoridad de Control propia en materia de protección de datos y es considerado por la Unión Europea un país con nivel adecuado de protección de datos personales, en virtud de la Decisión de la Comisión de 19 de octubre de 2010 [3], de conformidad con la Directiva 95/46/CE.

Su legislación en esta materia, desarrollada a partir del artículo 14 de su «Constitució del Principat d'Andorra» que data de 1993, está constituida, fundamentalmente, por una Ley y dos Reglamentos específicos[1]:

— Llei 15/2003, del 18 de desembre, qualificada de protecció de dades personals (LQPD).

— Decret d'aprovació del Reglament del registre públic d'inscripció de fitxers de dades personals, de 1 de juliol de 2004, con la corrección de erratas de 7 de julio de 2004 y cuyo anexo 1 fue rectificado mediante Decreto de 1 de octubre de 2008.

— Decret d'aprovació del Reglament de L'Agència Andorrana de Protecció de Dades (RAPDA), de 9 de juny de 2010, que deroga al de fecha 7 de julio de 2004 y que desarrolla especialmente los capítulos tercero, cuarto y séptimo de la LQPD.

BIEN JURÍDICO PROTEGIDO. DEFINICIÓN DE DATO DE CARÁCTER PERSONAL

El bien jurídico protegido por la legislación andorrana en materia de protección de datos es, a partir del artículo 14 de la «Constitució del Principat d'Andorra», el derecho de toda persona

---

[1] Portal de la Agència Andorrana de Protecció de Dades. Legislació d'Andorra. Normativa de Protecció de Dades.

a la intimidad y a ser protegida por las leyes contra las intromisiones ilegítimas en su vida privada, materializándolo en la tutela de los datos personales. En consecuencia, el contenido esencial en el derecho fundamental a la protección de datos se basa en un conjunto de reglas y principios de obligado cumplimiento para el que trata la información y que van dirigidas a proteger el dato personal considerado en sí mismo, a la vez que se limitan los tratamientos a que pueda ser sometido. Para ello se definen un conjunto de medidas preventivas de defensa que protejan a la información desde el mismo momento que se recaba y durante todo su ciclo de vida.

La regulación Andorrana en materia de protección de datos, según aparece en la exposición de motivos de la propia LQPD, busca el equilibrio entre tres objetivos fundamentales: primero, aportar un grado de protección que sea suficiente y razonable al derecho que toda persona tiene a su intimidad; segundo, que esta protección no implique el establecimiento de obligaciones excesivas que puedan impedir o dificultar gravemente las actividades económicas, administrativas o de gestión de las entidades públicas y privadas andorranas; tercero, aproximar la legislación andorrana a la normativa de su entorno en esta materia.

Según dispone el art. 2 LQPD «Esta Ley es aplicable a los datos de carácter personal que sean susceptibles de tratamiento y a cualquier uso posterior de estos datos».

INFORMACIÓN Y CONSENTIMIENTO. OBLIGACIÓN DE TRANSPARENCIA

En base al principio de transparencia, como lo entienden las autoridades europeas en su Dictamen 7/2009 sobre el nivel de protección de datos personales en el Principado de Andorra, las personas físicas deben recibir información sobre la finalidad del tratamiento que se pretende realizar sobre sus datos personales así como de la identidad del responsable de tratarlos, de los destinatarios si los hubiera de esos datos, de su derecho a no otorgar el consentimiento junto a las consecuencias derivadas de tal decisión y de los derechos ARCO que le asistirán durante todo el ciclo de vida de sus datos.

En este sentido, el derecho a la información de la persona interesada está regulado en los artículos 13 [sobre obtención de datos de la persona interesada] y 15 [Derecho de oposición] LQPD.

DATOS ESPECIALMENTE PROTEGIDOS Y OTROS TRATAMIENTOS INVASIVOS

La LQPD en su art. 3.11, define «datos sensibles» como aquellos datos referentes a opiniones políticas, creencias religiosas, pertenencia a organizaciones políticas o sindicales, salud, vida sexual, o origen étnico de las personas interesadas. Observamos que concuerda con los enumerados en el art. 8.1 de la Directiva 95/46/CE.

Partimos de que, cuando se traten categorías de datos sensibles, deben establecerse salvaguardias adicionales como el requisito de que la persona interesada otorgue su consentimiento explícito al tratamiento.

La legislación andorrana satisface este principio a tenor de lo dispuesto en los artículos 19 a 21 LQPD [relativos a datos sensibles, excepciones para el consentimiento expreso para datos sensibles y ficheros relativos a infracciones y sanciones penales o administrativas].

En concreto, el art. 19 LQPD establece que los datos sensibles solo pueden ser objeto de tratamiento o de comunicación con el consentimiento expreso de la persona interesada. Además, queda expresamente prohibida la creación de archivos con la finalidad exclusiva de recoger o tratar datos sensibles, con las excepciones que marque la Ley.

El RAPDA en su art. 8.1 dispone que en caso de duda, la prueba de la existencia del consentimiento de la persona interesada recae sobre el responsable del tratamiento. También se señalan las excepciones a la obtención del necesario el consentimiento de la persona interesada en el art. 8.2 RAPDA.

Dentro de la necesaria armonización en el ordenamiento jurídico andorrano y a modo de ejemplo, a satisfacción del grupo consultivo europeo del GT29 que así lo hace constar en su dictamen 7/2009[2], la Llei General de Sanitat, de 20 de marzo de 1989, modificada por la Llei 1/2009, de 23 de enero, en su texto refundido establece en su art. 69 ter la obligación, para todos los profesionales de la salud que ejerzan en territorio andorrano, de asegurar la confidencialidad de toda información nominativa y personal recibida en el marco de su praxis profesional.

Esta armonización sirve como garantía de aseguramiento frente a las excepciones para que sea necesario el consentimiento expreso antes del tratamiento de datos sensibles relativos a la salud, según dispone el art. 20 en las circunstancias e) y f). Como garantía adicional el art. 9 LQPD [sobre el secreto profesional], establece que esta Ley se aplica con carácter adicional a las normas reguladoras del secreto profesional, para las actividades y profesiones sujetas a esta obligación, normas reguladoras que en ningún caso se han de entender derogadas por esta Ley.

En relación a los tratamientos invasivos, en el art. 15 RAPDA se hace referencia a la toma de decisiones individuales, con efectos jurídicos, a partir de tratamientos automatizados.

CESIONES DE DATOS

Partiendo de que el art. 2.b) de la Directiva 95/46/CE define como tratamiento, entre otras funcionalidades, a «Cualquier operación (...), comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, (…)», avala que una cesión puede considerarse como una forma determinada de tratamiento y, en base al art. 17 LQPD, podemos inferir como norma general que los tratamientos de datos personales [incluyendo las cesiones] solo los pueden efectuar los responsables del tratamiento con el consentimiento inequívoco de las personas interesadas aunque con las excepciones que marca el art. 18 de la misma Ley.

En consecuencia, las cesiones de datos están íntimamente relacionadas con la obligación de informarlas al interesado y una vez enterado éste, si procede, con la subsiguiente posibilidad de ejercer el derecho de oposición.

El art. 15 de la Ley dispone que cualquier persona interesada tiene derecho a oponerse al tratamiento de sus datos por parte de un responsable del tratamiento, cuando éste no haya obtenido los datos directamente de la misma persona interesada. A estos efectos, cuando un destinatario de datos de carácter personal sea objeto de una comunicación de datos, dentro de un período máximo de 15 días a contar desde el momento en que recibe los datos, ha de informar de todas las circunstancias especificadas en las letras de la a) a la e) de ese art. 15 a las personas interesadas sobre las cuales haya recibido los datos y con las excepciones a la oposición que marca el art. 16 de esta misma Ley.

CALIDAD DE LOS DATOS

El principio de calidad de los datos determina que estos sean exactos y mantenidos actualizados durante todo su ciclo de vida. Está íntimamente relacionado con la aplicación del

---

[2] Grupo de Trabajo de Protección de Datos del Artículo 29. Documento WP 166. Dictamen 7/2009 sobre el nivel de protección de datos personales en el Principado de Andorra. Adoptado el 1 de diciembre de 2009.

principio de proporcionalidad, según el cual los datos deben ser adecuados, relevantes y pertinentes, sin rebasar la finalidad para la que inicialmente fueron recabados.

Este principio está recogido expresamente en el art. 11.b) LQPD, con arreglo al cual los datos objeto del tratamiento deben corresponderse con los datos personales reales de las personas interesadas, y que, a estos efectos, se tomen medidas para actualizarlos o suprimirlos.

En relación al principio de proporcionalidad debíamos de recurrir, antes del Reglamento de 2010, a la «Constitució del Principat d'Andorra de 1993» que, en su artículo 3.4 dispone que los tratados y acuerdos internacionales se integran en el ordenamiento jurídico a partir de su publicación en el «Butlletí Oficial del Principat d'Andorra», y no pueden ser modificados o derogados por las leyes. Concretamente nos referimos al art. 5.b) del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, «para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal», que establece que los datos personales objeto de tratamiento automático (…) deberán almacenarse para finalidades específicas y legítimas y no utilizarse de ningún modo incompatible con dichas finalidades, y al art. 5.c) del mismo Convenio 108 que prohíbe el tratamiento de datos que rebasen la finalidad para la que se almacenaron. Actualmente, tras la entrada en vigor del RAPDA, ya no se hace necesario recurrir al Convenio 108 al disponer en su artículo 6.3 que los datos deben ser adecuados, pertinentes y no excesivos en relación a las finalidades para las cuales son recabados y para las cuales posteriormente se tratarán.

HABEAS DATA Y DERECHOS ARCO

Entendemos por *habeas data* el derecho que se configura como un elemento propio de la autodeterminación informativa. Se trata de la facultad, por parte de una persona física, de poder controlar y decidir sobre el uso, propio y de terceros, de los datos de carácter personal a ella referidos. En otras palabras, el derecho de *habeas data* es el derecho que cada persona tiene de poder decidir sobre el uso que se hace de sus propios datos personales.

El *habeas data* se materializa en el derecho de acceso como mecanismo de verificación y control de los propios datos por parte del interesado, amparado por la legislación. Aquí aparecen también incardinados los demás derechos conocidos como ARCO por sus iniciales.

En el Principado de Andorra, el derecho de acceso viene recogido en el art. 22 de la LQPD, manifestando que cualquier persona interesada tiene derecho a ser informada por el responsable del tratamiento de sus datos que son objeto de tratamiento.

El derecho de rectificación está regulado en el art. 23 de la LQPD como el derecho que asiste a cualquier persona interesada para solicitar al responsable del tratamiento que los datos que son objeto de tratamiento sean corregidos, si son erróneos. La decisión debe ser comunicada al interesado y, si es denegada, debe estar motivada y será susceptible de ser recurrida delante de la jurisdicción competente.

El derecho de cancelación es designado en la LQPD como derecho de supresión. Se prevé en el art. 24 de la Ley como que cualquier persona interesada tiene derecho a solicitar al responsable del tratamiento que los datos que son objeto de tratamiento sean suprimidos.

El responsable dispone de tres supuestos de excepción para denegar la solicitud [Conservación de datos necesaria de acuerdo con una Norma vigente, conservación necesaria para cumplir con finalidades legítimas del responsable, y cuando la conservación sea necesaria en virtud de relaciones jurídicas u obligaciones contractuales]. En cualquier caso, delante de la denegación a la solicitud, que ha de estar motivada, el interesado podrá efectuar recurso contra dicha decisión delante de la jurisdicción competente.

MEDIDAS DE SEGURIDAD

Aunque las medidas de seguridad son de índole organizativa y técnica, no debemos olvidar que el bien jurídico protegido por el «principio de seguridad» es el núcleo esencial de la protección de datos: preservar el dato personal en si mismo. Esta protección ha de ser completa (recordemos que los tres atributos de la seguridad son: confidencialidad, integridad y disponibilidad) aunque atendiendo al principio de proporcionalidad. Podemos decir que el dato personal en si mismo junto al principio de seguridad, el principio de consentimiento informado y el *habeas data,* integran todo el contenido esencial de la protección de datos. El resto podríamos considerarlos elementos complementarios o de legalidad ordinaria.

En el Principado de Andorra el art. 12 LQPD dispone que los responsables del tratamiento han de establecer las medidas técnicas y de organización, necesarias para garantizar la confidencialidad y la seguridad de los datos personales que sean objeto de tratamiento. Igualmente, los responsables del tratamiento han de exigir a los «prestadores de servicios de datos personales» (encargados del tratamiento) el establecimiento de las medidas técnicas y de organización que el responsable del tratamiento considere mínimas, siempre que estas medidas mínimas se correspondan con las que el mismo responsable tenga establecidas para tratamientos de datos propios y de naturaleza análoga a los que sean objeto del servicio.

ENCARGADOS DE TRATAMIENTO Y *CLOUD COMPUTING*

Llama la atención, en el art. 3 LQPD y en el art. 5.10 RAPDA, que mientras en las definiciones se refiere al rol de «responsable del tratamiento» (en su idioma Responsable del Tractament), utiliza el término «prestador de servicios de datos personales» para referirse al rol de «encargado del tratamiento» (en su idioma Prestador de Serveis de Dades Personals). Entender la terminología empleada es importante a efectos de interpretar correctamente esta Ley.

Así, se define al prestador de servicios de datos personales como la persona física o jurídica, de naturaleza pública o privada, que, solo o conjuntamente con otros, trata los datos de carácter personal por cuenta del responsable del tratamiento, o que accede a los datos personales para la prestación de un servicio a favor y bajo el control del responsable del tratamiento, siempre que no utilice los datos a que tenga acceso para finalidades propias, o que no los haga servir más allá de las instrucciones recibidas o para finalidades diferentes del servicio que ha de prestar a favor del responsable.

Vemos que se invoca en la definición el principio de limitación de la finalidad, principio considerado como piedra angular de la protección de datos a futuro, debido a la tendencia de la humanidad hacia un uso masivo de Big Data y aplicación posteriormente a los datos de tratamientos analíticos. El propio GT29 hablaba en su dictamen WP203 del análisis necesario para poder determinar que estos tratamientos posteriores no sean «incompatibles» con la información facilitada en el momento del recabado inicial de los datos. Esta idea viene reforzada en el artículo 11.a) LQPD que establece que los tratamientos de datos personales solo los pueden llevar a cabo los responsables del tratamiento si reúnen, entre otros requisitos, que el tratamiento sea realizado para las finalidades previstas en la norma o en la decisión de creación de los ficheros de datos personales.

El art. 9 RAPDA exige que la prestación de servicios de datos personales han de estar regulados en un contrato escrito, que permita acreditar la concertación y el contenido, y habrá de establecer la manera expresa que el prestador de servicios solo debe tratar los datos de acuerdo con las instrucciones del responsable del tratamiento y que no los puede aplicar ni

utilizar con una finalidad distinta de la que figura en el contrato acordado, ni comunicarlas a otras personas, ni tan solo para conservarlas.

La evolución tecnológica actual y la preponderancia de los tratamientos de datos informatizados bajo el modelo de entrega de servicios conocido como *cloud computing*, por un lado, y la realidad de facto de que la mayoría de prestadores se encuentren fuera del territorio, por otro, han hecho que las transferencias internacionales de datos (TID) sean un aspecto muy importante a considerar en relación a la protección de datos personales. Pensemos que el prestador de servicios de *cloud computing* será considerado «prestador de servicios de datos personales» (encargado del tratamiento), siempre que llevemos al cloud datos de naturaleza personal.

En el Principado de Andorra se parte, según dispone el art. 35 LQPD, de que no se pueden efectuar transferencias internacionales de datos cuando el país de destino de los datos no establezca, en su normativa vigente, un nivel de protección para los datos de carácter personal equivalente, como mínimo, al que está establecido en esta Ley. Existen excepciones autorizadas en el art. 37, pero en total concordancia con el art. 26.1 de la Directiva europea 95/46/CE.

AUTORIDAD DE CONTROL. INSCRIPCIÓN O REGISTRO DE TRATAMIENTO. PROCEDIMIENTOS. SANCIONES

El capítulo séptimo de la LQPD crea la «Agència Andorrana de Protecció de Dades (APDA)»[3], organismo público con personalidad jurídica propia, independiente de las administraciones públicas y con plena capacidad de obrar. También los capítulos del séptimo al undécimo del RAPDA tratan sobre la APDA, centrándose el art. 23 en su ámbito de actuación, el art. 24 en sus competencias y el art. 25 en sus funciones, entre otros muchos temas de detalle. El Director de la Agéncia y los inspectores de protección de datos son designados por el «Consell General d'Andorra» por mayoría cualificada de dos terceras partes en primera votación (…), según dispone el art. 39 LQPD. La APDA se financia exclusivamente de las partidas que cada año establece para su funcionamiento el «Consell General d'Andorra» (vid. art. 39 LQPD).

Entre sus potestades está, entre otras y según dispone el art. 40 de la Ley y el art. 25 RAPDA, velar por el cumplimiento de la misma, gestionar el Registro Público de Inscripción de Ficheros de Datos Personales, publicar anualmente la lista de países con nivel de protección equivalente, ejercer potestad inspectora y sancionadora, proponer mejoras en la normativa de protección de datos, elaborar una memoria anual, emitir informes con carácter consultivo, atender las peticiones que le haga la ciudadanía y coordinarse con otras autoridades de control.

En el Principat d'Andorra, según dispone el art. 27 de la LQPD existe la obligación de inscripción de los ficheros de datos personales. Las personas físicas o jurídicas de naturaleza privada que sean responsables del tratamiento de datos, han de inscribir el fichero de datos personales bajo su responsabilidad, antes de crearlo, en el registro público gestionado por la autoridad de control. La creación, modificación o supresión de ficheros por parte de los organismos públicos deberá estar precedida por una Norma de creación, que ha de ser aprobada por la entidad pública responsable de su tratamiento, y que ha de ser publicada en el «Butlletí Oficial del Principat d'Andorra» antes de la creación, modificación o supresión del fichero, con las excepciones reflejadas en el art. 30 de esta Ley.

---

[3] Si bien la propia «Agència Andorrana de Protecció de Dades» se contrae el nombre como APDA, los organos judiciales andorranos en sus sentencias, como las referidas en este estudio, suelen referírsele como AAPD.

El art. 41 de esta Ley establece la posibilidad de que la Agencia inicie una inspección por propia iniciativa (de oficio) y siempre con autorización del Director de la APDA, o a solicitud de cualquier persona interesada (tutela de derechos) que considere que sus datos personales se han visto afectados o que un responsable ha infringido las obligaciones que impone la Ley.

La APDA tiene potestad sancionadora de acuerdo con el procedimiento establecido en el «Codi de l'Administració». En cuánto a las sanciones, tratadas en el capítulo quinto de la LQPD, se refieren al incumplimiento de sus disposiciones, estableciendo como principio general que el incumplimiento de esta Ley por parte de personas físicas o de personas jurídicas de naturaleza privada es objeto de sanción administrativa.

El primer incumplimiento por parte de un responsable de fichero se sanciona con una multa de importe máximo de 50000 euros, y los incumplimientos subsiguientes en que pueda incurrir el mismo responsable se sancionan con una multa de un importe máximo de 100000 euros, según dispone el art. 33 de la Ley. En los casos en que el responsable de los datos sea un organismo público, el art. 34 de la LQPD prevé que se apliquen el procedimiento y las sanciones establecidos en las disposiciones reguladoras de los regímenes disciplinarios.

Una peculiaridad de la legislación andorrana en materia de protección de datos es que no existe una lista detallada de incumplimientos junto a la sanción correspondiente para cada una de ellas. Se deja total libertad a la APDA para su cuantía teniendo en cuenta una serie de criterios. Esta indeterminación ha propiciado la Sentencia 31/2008 del Tribunal Superior de Justicia del Principat d'Andorra, Sala Administrativa, de 31 de marzo de 2008[4], que obliga a la APDA a individualizar primero la conducta infractora para evitar incumplir el principio de ne bis in ídem. Una vez hecho esto, según el alto tribunal, ya se modulará la sanción según los criterios establecidos en el art. 33 LQPD.

Cabe mencionar el art. 26 LQPD que recuerda que las sanciones previstas en el capítulo quinto de esta Ley se entienden sin perjuicio de la responsabilidad civil en que pudiera incurrir un responsable del tratamiento en caso de incumplimiento de la misma. Para recurrir las resoluciones de la APDA[5], el art. 44 LQPD establece que la APDA adecuará en todo momento su actuación al «Codi de l'Administració», las resoluciones de la cual serán impugnables conforme lo que se establece en dicho cuerpo legislativo. Debe tenerse en cuenta que, según dispone el art. 36.1 del RAPDA, las infracciones tipificadas en la Llei 15/2003, de 18 de desembre, qualificada de protección de dades personals (LQPD), prescriben al cabo de tres años de haberse cometido.

2.2 ARGENTINA

Constitución de la Nación Argentina

Artículo 43: Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

---

4 Sentencia 31/2008 del Tribunal Superior de Justicia del Principat d'Andorra, Sala Administrativa, de 31 de marzo de 2008.

5 Sentencia 39/2006 del Tribunal Superior de Justícia del Principat d'Andorra, Sala Administrativa, de 23 de noviembre de 2006.

BIEN JURÍDICO PROTEGIDO. DEFINICIÓN DE DATO DE CARÁCTER PERSONAL

En Argentina la protección de datos personales tuvo un proceso receptivo que se inició con las reformas de algunas Constituciones provinciales después del retorno del país a la democracia en 1983. En cambio en el ámbito nacional esta protección y el *habeas data* se instalan con la reforma de la Constitución Nacional de 1994[6]. La Convención reformadora introdujo el *habeas data* dentro de la primera parte de la Constitución, capítulo II, denominado «Nuevos derechos y garantías», en el art. 43, párr. 3.º, juntamente con el «amparo y el *habeas corpus*»[7].

El Párr. 3.º mencionado establece lo siguiente: «Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística» El párrafo transcripto de la C.N. no menciona expresamente los derechos tutelados, sino establece que funciona frente a los casos de «falsedad o discriminación», «para exigir la supresión, rectificación, confidencialidad o actualización de aquellos». Esta falta de especificación ha dado lugar a diversas interpretaciones, por un lado se ha opinado que sólo tutelaba el derecho a la intimidad y por otro que la tutela era más amplia abarcando tanto el derecho a la intimidad como a la imagen, el honor, la identidad, la libertad informática, la reputación[8].

No obstante con la sanción de la ley 25.326 de Protección de los Datos Personales[9] queda zanjada la polémica, pues su art. 1.º establece que el objeto de la ley es la protección integral de los datos personales y garantiza el derecho al honor y a la intimidad de las personas, como también el acceso a la información que de ellas se encuentre registrada en bases de datos públicos o privados. Incluye a las personas de existencia ideal. Así se ha expresado en jurisprudencia que «El bien jurídico protegido del *habeas data* es la veracidad de la información»[10].

Definición de dato de carácter personal: Art. 2.º de la ley 25.326: Definiciones— «Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables».

INFORMACIÓN Y CONSENTIMIENTO. OBLIGACIÓN DE TRANSPARENCIA

Los arts. 5.º y 6.º de la ley 25.326 se ocupan de regular el consentimiento y el deber de información al titular de los datos. El tratamiento de datos es lícito cuando el titular hubiera prestado su consentimiento libre, es decir como todo acto voluntario, debe ser prestado con discernimiento, intención y libertad, conforme lo establece el art. 897 del Código Civil Argentino; expreso e informado, por lo tanto inequívoco, descartando así toda posibilidad de que pueda ser tácito o presunto; deberá constar por escrito o por otro medio indubitable. El mismo art. 5.º de la ley indicada establece excepciones a la obligación de prestar el consentimiento por parte del titular de los datos cuando: a) los datos se obtengan de fuentes de

---

6 PUCCINELLI, OSCAR R.: «El *habeas data* en el constitucionalismo indoiberoamericano finisecular», En Toricelli, Maximiliano (coord.) El amparo constitucional: perspectivas y modalidades (art. 43, CN) Depalma, Bs. As., 1999. P. 249.

7 MARTÍNEZ MATILDE S.: *Habeas Data Financiero*. Ediciones de la República. 2009. P. 108/109.

8 PUCCINELLI, O. R.: *El habeas da*… cit. P. 255/258.

9 Ley 25.326, sancionada el 4/10/2000 (B:O: 2/11/2000) http: // infoleg.mecon.gov.ar.

10 CNAC, Sala B, en «Mimbielle, Carlos A. v. Banco Credicoop Cooperativo Ltdo.», 30/6/2005, JA 2007-IV-.

acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del art. 39 de la Ley 21.526. Dicho precepto trata acerca del secreto bancario, por el cual no se pueden revelar las operaciones pasivas de los clientes de entidades financieras.

Además el titular del dato personal cuando preste su consentimiento debe ser informado tal como lo dispone el art. 6.º de la ley señalada, de forma expresa y clara sobre la finalidad del tratamiento de los datos, los posibles destinatarios de la información, la existencia del banco de datos electrónico o de cualquier otro tipo, la identidad y el domicilio del responsable, el carácter obligatorio o facultativo de las respuestas que los requerimientos que se le realicen, las consecuencias que puede aparejar el proporcionar o no los datos, o hacerlo en forma inexacta, y la posibilidad de ejercer sus derechos de acceso, rectificación y supresión de los datos.

DATOS ESPECIALMENTE PROTEGIDOS Y OTROS TRATAMIENTOS INVASIVOS

A diferencia de la Ley Orgánica de Protección de Datos de Carácter Personal española[11], que refiere a «Datos especialmente protegidos», nuestra ley de protección de datos personales, en su art. 7.º señala como «Categoría de los datos» a aquellos que requieren una protección más adecuado a dicha clase.

Así prohíbe la recolección de datos sensibles. Estos se encuentran definidos en el art. 2.º de la ley 25.236, «Definiciones— Datos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.» En síntesis se trata de datos personales que por sus connotaciones contengan la actitud de generar conductas discriminatorias o vejatorias. Estos datos sólo podrán ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley o cuando haya finalidades estadísticas o científicas y sus titulares no puedan ser identificados.

Si bien queda prohibida la formación de bancos, archivos o registros que almacenen información que directa o indirectamente revelen este tipo de datos, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de los miembros con la finalidad de organizar su propia estructura, pero sin tener atribuciones para difundirlos. Asimismo, se establece que los datos relativos a antecedentes penales o contravencionales quedan sujetos a sus propias reglamentaciones.

CESIONES DE DATOS

El art. 11 de la LOPD reglamenta el tratamiento de la «cesión» de datos personales. Esto es, su transferencia, transmisión o comunicación[12]. En primer lugar, el artículo indicado establece que los datos de carácter personal objeto de tratamiento, sólo pueden ser cedidos con el interés

---

11 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España. Art. 7. BOE-A-1999-23750.

12 PEYRANO, GUILLERMO F.: *Régimen Legal de los Datos Personales y* Habeas Data. Lexis Nexis-Depalma.2002. P. 125.

legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario a los elementos que permitan hacerlo. Asimismo, el inc. 2 establece que el consentimiento podrá ser revocable. El inc. 3 dispone en qué casos no será necesario el consentimiento del titular de los datos para su cesión, siendo los siguientes: a) cuando así lo disponga una ley; b) en los supuestos previstos en el art. 5.º, inc. 2. Estos ya fueron tratados en este trabajo en el tema Información y consentimiento al que remitimos en honor a la brevedad; c) cuando se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; d) cuando se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de sus titulares, mediante mecanismos de disociación adecuados; e) cuando se hubiera aplicado un procedimiento de disociación, de modo que los titulares de los datos sean inidentificables. El inc. 4 prescribe que el cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias que el cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

Esta responsabilidad solidaria y conjunta, establecida expresamente por la ley está vinculada con el interés legítimo del cedente y del cesionario, y la exigencia de la norma ha sido lo suficientemente clara como para despejar cualquier duda que pudiera suscitarse al respecto. No obstante ello, el decreto 1558/2001[13] reglamentario de la ley 25.326 ha dispuesto que el cesionario a que se refiere el art. 11, inc. 4, de la ley 25.326, podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño. Como se puede observar el decreto ha modificado los términos tan expresos y contundentes del inciso en comentario. No obstante, sabemos que los decretos reglamentarios, por el imperio de la Constitución Nacional, no pueden alterar el espíritu de las leyes con excepciones reglamentarias conforme lo establece el art. 99, inc. 2 de la CN[14]. Por lo tanto la disposición del decreto en comentario resulta ilegal e inconstitucional[15].

CALIDAD DE LOS DATOS

En la ley de protección de datos personales la calidad de los datos se encuentra regulada en el art. 4.º estableciendo en el inc. 1. que los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos con relación al ámbito y finalidad para los que se hubieran obtenido. El inc. 2. dispone que la recolección de los datos no podrá hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la LPDP.

Se refiere a la lealtad y buena fe con la que deben obrar los responsables de bancos o archivos, en todas las fases del tratamiento de datos personales[16]. En el inc. 3. Establece que los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Ello está relacionado con el «principio de pertinencia de los datos[17].

El inc. 4. señala que los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario y el inc. 5. indica que los datos total o parcialmente inexactos, o que sean incompletos,

---

13 Decreto 1558/2001. http://www.infoleg.mecon.gov.ar.
14 MARTÍNEZ, M.S.: *Habeas Data…,* cit. P. 159/160.
15 PEYRANO, G.F.: *Régimen…,* cit. P. 140/141.
16 MARTÍNEZ, M.S.: *Habeas Data…,* cit. P. 149.
17 GOZAÍNI OSVALDO A.: *Derecho Procesal Constitucional.* Habeas data. *Protección de datos personales.* Ley 25.326. 1.ª ed., Rubinzal-Culzoni, Bs.As.. 2002. P. 51.

deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el art. 16 de la ley, es decir rectificación, actualización, supresión o confidencialidad.

Entonces, de acuerdo a lo dicho por la ley los datos deben ser «ciertos», es decir verdaderos, también exactos y deben ser actualizados cuando ello sea necesario. La determinación de la veracidad, exactitud o actualidad deberá ser el producto de la verificación de la realidad de la porción de la información que el mismo representa de su titular[18]. Como vimos los datos además deberán ser «adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieran obtenido».

Adecuación, pertinencia y no excesividad se consideran como el «principio de proporcionalidad», es decir que los datos personales recogidos y almacenados deberán responder estrictamente a la finalidad para la cual fueron recolectados[19].

La ley pone en cabeza del responsable del archivo, cuando tengan conocimiento, la obligación de la exactitud, completitud, adecuación, pertinencia, no excesividad, de los datos. Asi la Corte Suprema de Justicia de la Nación ha expresado que «los datos registrados por las empresas que prestan servicios de información crediticia deben ser exactos y completos[20].

Asimismo, el inc. 6. determina que los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Y por último, el inc. 7. Ordena que los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

HABEAS DATA Y DERECHOS ARCO

Tal como lo habíamos tratado el art. 43, 3.er párr. de la CN. garantiza el derecho de acceso a los titulares de los datos personales a ellos referidos, almacenados en archivos o bancos de datos públicos y privados destinados a proveer informes, complementándose ésta con la garantía del derecho a exigir la supresión, rectificación, confidencialidad o actualización de los datos, ante cualquier incumplimiento de acuerdo lo analizado en calidad de los datos o ante la violación de la LPDP.

La ley 25.326 regula esta garantía ocupándose el art. 14 del derecho de acceso al titular de los datos y el art. 16 de la misma ley reglamenta el derecho de rectificación, actualización y supresión de los datos. La ley indicada reglamenta el ejercicio del *habeas data* a través de dos procesos, uno prejudicial, tanto para el derecho de acceso como para el derecho de rectificación, actualización y supresión de los datos y otro proceso judicial. Es decir que si el titular de los datos no queda satisfecho con el resultado del proceso prejudicial, le queda la vía expedita para iniciar la acción judicial de *habeas data*[21]. En los preceptos señalados se establecen todos los requisitos de ambos procesos.

MEDIDAS DE SEGURIDAD

Los art. 9.º y 10 de la ley 25.326, establecen que el responsable o usuario de archivos o bases de datos deben adoptar las medidas técnicas y de organización para garantizar la

---

18 PEYRANO, G.F.: *Régimen…,* cit. P. 61.
19 GOZAÍNI O. A.: *Derecho Procesal…,* cit. P. 51.
20 CSJN. «Martínez, Matilde Susana c. Organización Veraz SA.» Fallos 328.927. 05/04/2005.
21 Ver in extenso en: MARTÍNEZ, M.S., Habeas Data….cit. P 229/260.

seguridad y la confidencialidad de los datos personales. Es obligación de éstos evitar la adulteración, pérdida o consultas no autorizadas de los datos. Además, los mecanismos técnicos o humanos utilizados, deberán permitir la detección de posibles desviaciones de datos, sean éstas intencionales o no.

Conforme al Decreto reglamentario 1558/2001, quedan a cargo de la Dirección Nacional de Protección de Datos Personales el control y verificación del cumplimiento de esta obligación. La mencionada Dirección, a través de la disposición 11/2006[22] ha aprobado las Medidas de Seguridad y Conservación de los Datos Personales en Archivos, Registros, Bancos y Bases de Datos Públicos no Estatales y Privados. Se establecen tres niveles de seguridad: básico, medio y crítico, de acuerdo a la naturaleza de la información tratada para todos los archivos (informatizados o manuales) indicándose las pautas para cada uno de los niveles. En cuanto a la confidencialidad de los datos la LPDP exige que todos los responsables, usuarios o personal que intervenga en cualquier parte del proceso del tratamiento de los datos quedan obligados a guardar secreto profesional y la obligación subsistirá aún finalizadas las relaciones.

ENCARGADOS DE TRATAMIENTO Y *CLOUD COMPUTING*

En Argentina no tenemos una regulación específica acerca de los servicios de *cloud computing* o computación en la nube, es decir esta nueva tecnología con la que podemos tener todos nuestros archivos e información en internet pudiendo acceder a ellos desde cualquier ordenador y sin necesidad de tenerla almacenada en nuestro espacio, debemos encuadrarlo siempre que se trate de almacenamiento de datos personales, dentro del marco de la Ley de Protección de los Datos Personales. Para ello el art. 25 de dicha ley regula la prestación de servicios informatizados de tratamiento de datos personales por cuenta de terceros estableciendo que no podrán utilizarse con fines distintos de los que figuren en el contrato celebrado entre el responsable del tratamiento y el encargado sobre la prestación del servicio y no podrán cederse ni para su conservación.

Además, en la reglamentación del decreto 1558/2001 se dispone que en el contrato mencionado deberá constar el cumplimiento de los niveles seguridad, confidencialidad y reserva de los datos que establece la ley. Agrega que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento y que las obligaciones del art. 9.º de la ley 25.326 incumben también al encargado del tratamiento, es decir las medidas de seguridad analizadas en dicho título de este trabajo. También queda establecido por la ley que una vez cumplida la prestación contractual, los datos personales tratados deberán ser destruidos, excepto que medie autorización expresa del responsable del archivo para que se los conserve por un período no mayor a dos años, cuando se presuma razonablemente que pueden ser objeto de ulteriores contrataciones.

AUTORIDAD DE CONTROL. INSCRIPCIÓN O REGISTRO DE TRATAMIENTO. PROCEDIMIENTOS. SANCIONES

El art. 29 de la ley 25.326 establece las normas que rigen al órgano de control, el cual deberá velar por el cumplimiento de las disposiciones de la ley y aplicar las sanciones civiles y

---

[22] Disposición DNPDP 11/2006 del 19/9/2006, publicada en el B.O. del 22/9/2006. http://www.jus.gov.ar/dnpdp/.

penales que la misma dispone, e indica las atribuciones y funciones de este órgano. A estos efectos, el decreto reglamentario 1558/2001 crea la Dirección Nacional de Protección de Datos Personales, en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos.

El Capítulo IV de la LPDP en los art. 21 a 28 se ocupa de los «Usuarios y Responsables de Archivos, Registros y Bancos de Datos» En primer término se establece que todos los archivos, bases o bancos de datos públicos y privados destinados a proveer informes, deben inscribirse en el registro habilitado por el organismo de control, éste es la Dirección Nacional de Protección de Datos Personales.

Para el cumplimiento de esta obligación deberán consignar, como mínimo, la siguiente información: nombre y domicilio del responsable; características y finalidad del archivo; naturaleza de los datos personales contenidos en cada archivo; forma de recolección y actualización de los datos; destino de los datos y personas físicas y de existencia ideal a las que pueden ser trasmitidos; modo de interrelacionar la información registrada; medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; tiempo de conservación de los datos; forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para rectificación o actualización de los datos. Para los archivos, registros o bancos pertenecientes a organismos públicos, su creación, modificación o supresión, deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial. En caso de supresión de los registros informatizados también se deberá consignar la forma de destrucción.

A su vez el órgano de control en el cumplimiento de sus funciones, mediante el dictado de la disposición 2/2003[23] del 20/11/2003 y sus complementarias habilitó el Registro Nacional de Bases de Datos donde se aprueban los formularios de inscripción al mismo y disponen la realización del Censo Nacional de Bases de Datos, con carácter obligatorio. La disposición 6/2005[24] del 1/9/2005 crea el diseño del isologotipo que identificará a los responsables de bases de datos inscriptos en el registro, quienes una vez aprobados los trámites pertinentes podrán hacer uso de aquel.

El régimen de sanciones se encuentra normado en los arts. 31 y 32 de la LPDP para los casos de incumplimientos y violaciones a dicha ley. En primer lugar se establece que el órgano de control podrá aplicar sanciones de: a) apercibimiento; b) suspensión; c) multas entre $ 1.000 y $ 100.000; d) clausura, o e) cancelación del archivo, registro o banco de datos.

Las mismas serán aplicadas sin perjuicio de las responsabilidades administrativas que correspondan en el caso de responsables o usuarios de bancos de datos públicos y de la responsabilidad por daños y perjuicios derivados de la inobservancia de la ley, y más allá de las sanciones penales previstas. El decreto reglamentario establece que la cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a los terceros y a cualquier otra circunstancia que sea relevante para la determinación.

---

23 http://www.infoleg.gob.ar/infolegInternet/anexos/90000-94999/90557/norma.htm- 9/8/2014.

24 http://www.infoleg.gov.ar/infolegInternet/anexos/105000-109999/109496/norma.htm- 9/8/2014.

Asimismo, establece las normas de procedimiento a las cuales se deberán ajustar para la aplicación de las sanciones dispuestas. En cuanto a las sanciones penales, el art. 32 de la LPDP incorpora los arts. 117 bis[25] y 157 bis[26] en el Código Penal Argentino.

2.3 CHILE

Constitución Política de la República de Chile

Artículo 19: La constitución asegura a todas las personas: 4.º El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.

En Chile se ha planteado recientemente una modificación Constitucional para elevar a la Carta Magna la disposición que se refiera directamente a la protección de los datos personales[27]. Así entonces, se pretende reconocer la acción *habeas data* u otra garantía específicamente diseñada que proteja los derechos de los titulares de los datos personales. Lo señalado se incorporaría a las disposiciones referidas a la protección de los bienes jurídicos vida de la privada e intimidad, en los cuales se podría fundamentar una tutela a los derechos de las personas en la materia de estudio.

El Ministerio de Economía de Chile elaboró una propuesta de ley con el fin de avanzar en la legislación de datos para cumplir con los estándares internacionales y así contribuir a un mejor desarrollo de las actividades económicas. El proyecto legislativo contiene un nuevo enfoque que va desde la regulación de un mercado de datos personales a la protección de las personas Para elaborar el anteproyecto de ley se consideró la legislación internacional, en especial la Resolución de Madrid, las Directrices de la Unión Europea y la OCDE y la experiencia de países como México, Costa Rica y Uruguay.

La iniciativa legal junto con fijar las condiciones para el tratamiento de datos, establece un sistema de derechos para las personas y crea mecanismos efectivos para hacerlos valer. Además crea una Autoridad de Protección de Datos, así como un régimen de sanciones para quienes no respetan la normativa.

---

25 Artículo 117 bis. C.P: 1.º (Inciso derogado por art. 14 de la Ley N.ª 26.388, B.O. 25/6/2008)
2.º La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.
3.º La escala penal aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.
4.º Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena. (Artículo incorporado por el art. 32 de la Ley 25.326 BO 2/11/2000/) http://www.infoleg.gov.ar

26 Artículo 157 bis. C.P: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
1.º A sabiendas e ilegítimamente proporcione, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2.º Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3.º Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años. (Artículo sustituido por art. 8.º de la Ley 26.388, BO 25/6/2008). http://www.infoleg.gov.ar

27 http://www.harboesenador.cl/2014/senadores-harboe-larrain-lagos-weber-tuma-y-araya-presentan-proyecto-de-reforma-constitucional-que-protege-los-datos-personales, 12/07/2014.

Actualmente la Ley 19.628 sobre protección de datos de carácter personal, de 1999, dispone sobre el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares. Define su texto «datos personales» como los relativos a cualquier información concerniente a personas naturales, identificadas o identificables, y «datos sensibles», como aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Por su parte, definió como «tratamiento de datos», cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma. La ley, en resumen, impone la autorización previa y escrita del titular para cualquier tratamiento de sus datos personales, le otorga a dichos titulares una serie de derechos y garantías (modificación, bloqueo, eliminación de los datos) y hace responsable a la persona natural o jurídica que administra los datos de los daños materiales y morales que pudiese causar en caso de incumplimiento.

BIEN JURÍDICO PROTEGIDO

La determinación de los bienes jurídicos por la legislación Chilena sobre protección de datos personales ha sido compleja por los autores en el sistema jurídico chileno, que en último término tiene su base en la Constitución Política de 1980.

La doctrina y los integrantes del poder legislativo que discutieron la ley, incluyeron como bien jurídico protegido a la vida privada, la intimidad, el honor, e incluso un derecho a la identidad, hasta postular directamente que se estaría frente a un derecho implícito, el denominado derecho a la autodeterminación informativa[28].

En este punto lo que efectivamente no está presente en la legislación chilena es la autodeterminación informativa[29]. El flujo de información a través de los constantes avances tecnológicos y la disponibilidad de soluciones para la «captura de datos en distintos tipos de dispositivos» para su tratamiento, ha despertado la precaución de quienes creen ver en ello un serio riesgo para los derechos fundamentales, desde que permite a quien dispone de la información acceder a partes de la vida que legítimamente debieran tenerse a resguardo y aun servirse de ella para condicionar el ejercicio de nuestras libertades. Cabe mencionar aquí que existe en Chile una incipiente Ley sobre Delitos Informáticos.

INFORMACIÓN Y CONSENTIMIENTO. OBLIGACIÓN DE TRANSPARENCIA

La generalidad en el ordenamiento jurídico chileno indica que debe cumplir con el consentimiento expreso del titular de los datos personales para que sea legítimo, al menos, su tratamiento. Sin embargo existen diversas excepciones legales lo que permite cierto grado de formalidad pero carente contenido y sentido.

La revisión de la norma permite identificar que el tratamiento de datos personales solo podrá efectuarse por la autorización de la ley, en comento, o por el consentimiento «expreso»

---

28 http://www.redalyc.org/pdf/820/82030204.pdf, Conceptualización, 10/07/2014.

29 Autodeterminación informativa y leyes sobre protección de datos Alberto Cerda Silva. Disponible en: http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/view/10661/11413, 19/07/2014

del titular, donde el propósito debe ser explícito y por escrito, lo que no es ampliamente de uso ni conocido por las personas. Otras figuras del mismo articulado son evidentemente confusas en materia de encuestas, estudios de mercado y otras formas de «recolección de datos». Así tal como se presenta el legislador chileno exige un mínimo deber información por parte de quien recolecta datos personales respecto del titular de éstos[30].

Ahora bien existen aspectos de la legalidad chilena que establecen algunas «excepciones» que están categorizadas en lo que para esta legislación trata como dato sensible, por ejemplo. Esta categoría de datos, es definida por la ley como aquellos datos personales «que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual».

La ley chilena en su intento de calificación confunde ya que señala[31] que: «no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares», en ella la intención es la prohibición de tratamiento de los datos sensibles, sin embargo el cuestionamiento podría estar el para establecer u otorgar beneficios de salud a los titulares de los datos, no dejando claro si estos pueden extenderse a otro tipos de datos sensibles. En este sentido y bajo la línea de varios autores locales el principio general en materia de procesamiento de datos personales, atendidas las excepciones que consagra, «no es sino una mera declaración de principios[32].

En suma, de lo anteriormente señalado se desprende que si bien la regla general en el ordenamiento jurídico chileno es el principio del consentimiento expreso del titular de los datos personales para que sea lícito el tratamiento de éstos, dadas las diversas excepciones que la Ley establece en la materia, éste se traduce en un principio meramente formal carente de contenido.

DATOS ESPECIALMENTE PROTEGIDOS Y OTROS TRATAMIENTOS INVASIVOS

Se encuentran especialmente protegidos los datos personales denominados sensibles, los que, por regla general, no pueden ser objeto de tratamiento.

Las críticas a la legislación existente es ampliamente expuesta ya que dada su naturaleza no es una herramienta eficaz para la protección de los datos personales. Es claramente visible en distintos ámbitos, como entre empresas, prensa y otros medios que estos circulen libremente. Con las prácticas actuales es posible crear con información personal, económica e incluso con los datos sensibles perfiles y otro tipo de información útil[33].

Algunos lo atribuyen a que la autorización del titular de los datos personales para su tratamiento, si es que se solicita, no ha sido implementada por la existencia de una amplia gama de excepciones que contempla la misma y con muy pocos derechos legales que permitan a dichos titulares denunciar, reclamar y hasta ser compensados.

---

30 Existe una mínima obligación de información (Arts. 3.º y 4.º Ley 19.628, pero considera solo una mirada de la buena fe).

31 Art. 10 Ley 19.628.

32 JIJENA LEIVA, R.: «La Ley Chilena de Protección de Datos Personales. Una visión crítica desde el punto de vista de los intereses protegidos», *Cuadernos de Extensión Jurídica,* Universidad de Los Andes, n.º 5, 2001, pág. 100.

33 En este sentido no hay referencia aquí a las redes sociales. Nota del Autor.

CESIONES DE DATOS

Es claro en este sentido solo señalar que no existe sanción penal sobre la cesión de datos personales cuando esta ocurre fuera de los parámetros de la ética o atentan contra los principios básicos de intimidad, privacidad y la honra. Si bien el legislador chileno «intenta dar forma» a la regulación sobre esta materia no es claro el límite de dicha cesión entre el titular, el que recoge los datos y un tercero, considerando además que no es explícito en la actual Ley.

CALIDAD DE LOS DATOS

Totalidad, integridad y disponibilidad de los datos[34] debiera ser consistente con el sentido que quiere dar el legislador a este principio. En Chile no está claramente definida y se intenta dibujar con una aproximación en su articulado de la Ley 19.628, con una clasificación referida a su cancelación o eliminación, bloqueo, la finalidad de su recolección, la publicación de datos financieros y económicos, la responsabilidad de organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias y finalmente sellando dicha definición reconocer el principio de la calidad de los datos al definir en la Ley lo que entiende por dato caduco.

Podría entonces señalar que los datos personales objeto de tratamiento manual o automatizado deben ser exactos, actualizados y veraces, pero sin una definición clara como pueden aparecer en otras legislaciones Iberoamericanas.

HABEAS DATA Y DERECHOS ARCO

Los derechos de los titulares de los datos y que son reconocidos por nuestra normativa son por su naturaleza[35]: información, cancelación, bloqueo, copia gratuita, aviso a terceros y oposición. Es posible desde la perspectiva de la intencionalidad del legislador que el concepto está, pero no se aplica ya que el recurso de *habeas data* en Chile ni para el público en general, ni los propios abogados están o son capaces de enfrentar una situación jurídica de esta naturaleza, tal vez por la baja sanción o por el uso y costumbre de la no reclamación ante el tratamiento abusivo de nuestros datos personales, ya sea por organismos públicos o privados.

Si bien se requieren modificaciones, la idea es que el recurso y su existencia se transforme en una herramienta eficaz y oportuna para evitar el uso indebido, sobre todo por aquellos que lo realizan con el argumento del «derecho de libertad de opinión e información» o aquellos propios de la ética al difundir datos personales de manera para denostar entre otros adjetivos.

MECANISMOS DE CONTROL

La legislación chilena de protección de datos personales, por ahora, no contempla la creación un órgano de control que vele por el resguardo de los derechos consagrados en ella, y que supervise la gestión de los responsables de los registros o bancos de datos de carácter personal. El único órgano al cual la ley de protección de datos personales chilena le encomienda alguna función relacionada con el tratamiento de esos datos es el Servicio de Registro Civil, el

---

34 Definición de la propiedad de los datos bajo el concepto de seguridad de la información.

35 http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewFile/10644/10906.

cual debe mantener un Registro de todos los bancos de datos personales a cargo solamente de organismos públicos (art. 22 de la ley en comento).

Sin embargo dicho Servicio (Registro Civil), no posee facultades coactiva respecto de los responsables de los bancos de datos a cargo de organismos públicos, por lo que no puede obligar a éstos a que inscriban sus bases de datos, es decir, su rol queda reducido a ser un ente meramente registral.

La falta de un órgano de control en la materia, quita fuerza y coherencia al sistema de protección de datos chileno, pero las autoridades actuales han visto esto como un elemento de modernización. Es en cualquier caso extraño, al menos, que se obligue inscribir los bancos de datos a cargo de organismos públicos y se deje fuera a los que están bajo la responsabilidad de privados o particulares.

Ciertamente este es un tema pendiente y mientras no se resuelva, nuestra legislación carecerá de una efectiva supervisión y control, donde cada banco de datos privado y sus responsables operarán en el «tráfico de datos personales» literalmente.

Hasta ahora entonces el que los legisladores chilenos no puedan imponer ante los privados la creación de un registro de bancos de datos personales, ni la obligación de inscribirlos por los particulares que sean responsables de esos bancos de datos poco se podrá avanzar para lograr una efectiva protección de los derechos de las personas sobre la identificación del registro o banco de datos, así como su finalidad, contenido y personas responsables de éste, dificultando finalmente el ejercicio de los derechos de información, modificación, cancelación y bloqueo de datos personales, al menos.

OTRAS NORMAS RELACIONADAS

Código Sanitario[36] Los datos personales relacionados con la salud de las personas pueden ser tratados en los casos que los «pacientes» lo autoricen, cuando los datos sean necesarios para la determinación u otorgamiento de beneficios de salud o en aquellos casos que sea necesario salvaguardar el interés vital de sus titulares en la hipótesis de que se encuentren física o jurídicamente imposibilitados de otorgar su consentimiento.

También se aborda el uso de las recetas médicas y exámenes de laboratorios clínicos y servicios relacionados con la salud, se califican de reservados, exigiendo para revelar su contenido o dar copia de ellos el consentimiento expreso y por escrito del titular de los datos (paciente). La pregunta es cuando el dato es necesario para un beneficio de salud o cuando se está imposibilitado de otorgar consentimiento.

La Ley 20.575[37] establece el principio de «finalidad en el tratamiento de datos personales», con el fin de asegurar que los sistemas de registro de deudas sean usados para la evaluación de riesgo comercial y para el proceso de crédito, y podrá ser dada a conocer sólo al comercio establecido y a las empresas que se dedican a la evaluación de riesgo.

El Código Tributario[38] establece lo que se denomina secreto tributario o fiscal, el cual resguarda las informaciones relativas a la fiscalidad de los contribuyentes.

---

36 Código Sanitario Decreto con fuerza de Ley n.º 725, disponible en http://bcn.cl/1m197.
37 http://bcn.cl/1m6tm.
38 http://bcn.cl/1m091.

Ley General de Bancos[39] hace referencia al denominado «secreto bancario», donde no podrán proporcionarse antecedentes relativos a dichas operaciones sino a su titular o a quien haya sido expresamente autorizado por él o a la persona que lo represente legalmente.

Código del Trabajo[40]. Sobre la reserva toda información y datos privados del empleador a los cuales ha tenido acceso con ocasión de la relación de trabajo.

Telecomunicaciones. La Ley 19.223[41] sobre Delitos Informáticos que data de 1993 y que ya se ha señalado que es una norma obsoleta y no está de acuerdo al uso que se da a la información y datos a su obtención, tratamiento y difusión no autorizada.

VISIÓN DE FUTURO: EL ANTEPROYECTO DE LEY TRATAMIENTO DE DATOS PERSONALES CHILE

En mayo del 2010 Chile firmó el Convenio de Adhesión a la Organización para la Cooperación y el Desarrollo Económico (OCDE) comprometiéndose entre otros aspectos, a subsanar las recomendaciones referidas sobre protección de la privacidad y flujo transfronterizo de datos personales, materias, entre otras, ausentes en la Ley n.º 19.628. Esto dio como resultado algunas iniciativas legislativas, pero no suficientes a las realidades internacionales en estas materias.

La actual administración tomando en cuenta la importancia de estas debilidades de la Ley Chilena, en materia de datos personales, ha elaborado un Ante Proyecto para «dar forma a un sistema de protección de datos sustentado en el derecho de las personas de controlar y proteger su información, de manera de evitar que sus derechos sean afectados por el tratamiento de datos»[42].

Estos principios orientadores, según las propias autoridades del Ministerio de Economía de Chile, recogen la experiencia y la discusión nacional que se ha dado en el Congreso Nacional[43]y en los Tribunales de Justicia, de manera de adaptar la legislación a los estándares internacionales de protección de datos.

Para la elaboración del Proyecto de Ley se tomaron como base la «Resolución de Madrid», la Directiva de la Unión Europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, las Directrices de la OCDE relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales, la Ley Orgánica 15/1999 de España de Protección de Datos Personales, la Ley Estatutaria de Colombia n.º 1581 por el cual se dictan disposiciones generales para la protección de datos personales, la Ley n.º 8968 de Costa Rica de Protección de la persona frente al tratamiento de sus datos personales y la Ley 18.331 de Uruguay sobre protección de datos personales. Adicionalmente, se consideró el texto del Reglamento de la Unión Europea que está en revisión, de acuerdo a como lo indica la entidad de Gobierno.

De acuerdo a la información disponible la base y principio tendrá énfasis en proteger a las personas en cuanto al uso de sus datos personales, de manera tal que una persona pueda conocer cuál es la información que tiene de ella una entidad, empresa o casa comercial y de esa forma, poder dar forma legal a los denominados derechos ARCO. Por lo pronto uno de los

---

39 http://bcn.cl/1m3ab.
40 http://bcn.cl/1lyoh.
41 http://bcn.cl/1m196.
42 http://www.participacionciudadana.economia.gob.cl/consultas-ciudadanas-virtuales/ante-proyecto-de-ley-proteccion-de-las-personas-del-tratamiento-de; 05/10/2014.
43 Parlamento Chileno.

elementos más significativos es la idea de legislar para la creación de una Entidad de Control que permita un uso eficiente del costo de protección de estos datos y que exista una instancia de sanción efectiva sobre el mal uso de los datos personales.

Este organismo tendrá entre sus facultades (similares a las que aborda la autoridad en su estudio comparado), realizar actividades de difusión e información al público sobre protección de datos; autorizar el funcionamiento de bases de datos cuando corresponda; dictar instrucciones que permitan a los organismos públicos, privados y personas naturales adecuar los tratamientos de datos a la ley; fiscalizar el cumplimiento de la legislación, general y especial, sobre protección de datos; ejercer la potestad sancionadora; resolver los reclamos por infracciones a la ley; ordenar la eliminación de las bases de datos, cuando no se ajusten a la ley; mantener un Registro Nacional de Bases de Datos en el que se deberán inscribir todas las bases de datos de titularidad pública y privada que cumplan con las exigencias para su inscripción; entre otros.

La propuesta del Ejecutivo otorga un capítulo específico al tratamiento de datos sensibles y a las transferencias internacionales[44].

La iniciativa pretende un cambio respecto de la protección desde la regulación de «un mercado de datos personales» a la protección de las personas. Con esto es factible inducir que las autoridades chilenas tienen una visión concreta respecto de la realidad internacional en estas materias, sin embargo no debiesen perder de vista la realidad de las Tecnologías de la Información, las redes sociales y el almacenamiento en Internet, como asimismo el excesivo proteccionismo que suele incorporar algunas barreras técnicas a los emprendimientos por ejemplo.

CONSIDERACIONES FINALES

Es indudable que Chile debe asumir que la legislación nacional sobre la materia tiene dificultades en lo que se refiere al estándar internacional, debiendo incorporar una serie de modificaciones a la legislación con miras a lograr el cumplimiento de dichos marcos.

La inadecuada forma en que los organismos públicos y privados, como consecuencia de la pasividad legal normativa, tratan los datos personales permite que los ciudadanos vean hasta con algo normal el que se pueda hacer cualquier cosa con la información de las personas sin considerar, ni conocer que se afectan con ello, derechos fundamentales, como vida privada la honra y otros derechos asociados.

2.4 COLOMBIA

Constitución Política Colombiana

Artículo 15: 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 los 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.

---

[44] Asunto pendiente de modificación en la Ley chilena y observado por la OCDE.

Para el caso colombiano, lo relativo a protección de Datos Personales – *Habeas Data,* ha sido un tema recurrente desde 1991, y tiene su raíz y piedra angular en un precepto Constitucional esbozado en el Art. 15 de la carta política de ese año, donde es elevado a rango máximo y establecido como un derecho fundamental, a través del cual, todo individuo tiene el derecho a conocer, actualizar y rectificar todo tipo de información que se haya recogido sobre él o que haya sido objeto de tratamiento en bancos o bases de datos electrónicas o no, y en general en archivos de entidades públicas y privadas. Así mismo, vale decir que existen una serie de aristas, y normas sobre otros temas, que orbitan a su alrededor y complementan el espectro normativo en nuestro entorno.

Como hemos mencionado, el Art. 15 de la Constitución Colombiana define el derecho de *Habeas Data* como: «Artículo 15. 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».

FINALIDAD DEL DERECHO FUNDAMENTAL DE *HABEAS DATA*

Sin duda la razón de ser, y el sustrato del derecho fundamental para el manejo y protección de Datos Personales – *Habeas Data,* es el derecho que le asiste a todo individuo, persona natural a conocer, actualizar y rectificar todo tipo de información que se haya recogido sobre ella o que haya sido objeto de tratamiento de datos personales en bancos o bases de datos y en general en archivos de entidades públicas y privadas; de manera particular de acuerdo con lo consignado en el Art. 15 de la Constitución, en Ley estatutaria n.º 1266 de 2008, Decretos Reglamentarios Decreto 1727 de 2009 y Decreto 2952 de 2010; la ley estatutaria n.º 1581 de 2012; las Sentencias de la Corte Constitucional C – 1011 de 2008, y C – 748 del 2011; los Decretos reglamentarios n.º 1377 de 2013 y Decreto n.º 886 de 2014 y demás normas complementarias que las adicionen o modifiquen; buscan que los titulares de derechos, tengan claridad sobre las pautas sobre su información, privacidad, seguridad, manejo y tratamiento de datos personales.

Lo anterior se traduce en lo que a nivel mundial se conoce como los principios o DERECHOS ARCO, y que la doctrina y la jurisprudencia han desarrollado como los derechos de Acceso, Rectificación, Cancelación y Oposición.

PRINCIPIOS GENERALES Y POSTULADOS

Las distintas fuentes del derecho de *habeas data* que se tienen en el escenario Colombiano, tienen como soporte y cimiento unos principios generales, tales como la buena fe, la legalidad, la autodeterminación informática, la libertad y la transparencia, que son una premisa constante en la recolección, manejo, uso, tratamiento, almacenamiento, circulación e intercambio; que en su aplicación permitan garantizar la protección del derecho fundamental de *Habeas Data,* pudiendo conocer, actualizar y rectificar todo tipo de información recogida en bases o bancos de datos, bien sea de quien actúa como Encargado del Tratamiento, o Responsable del Tratamiento de todo tipo de datos personales, tales como datos comerciales y financieros, datos laborales, académicos, de salud, penales, tributarios, incluyendo los denominados datos sensibles y cualquier otra clase de dato que a futuro sea catalogado como dato personal.

Por ello es un deber y una constante, el que subyacente a la protección del derecho fundamental de *habeas data* y tratamiento de datos personales; garantizar la defensa y buen uso del grueso de derechos fundamentales que puedan verse inmerso en esta clase de relación,

tales como los derechos a la privacidad, la intimidad, el buen nombre, la imagen, la autonomía universitaria, y en general toda clase de derecho fundamental, y los derechos humanos.

Principio de Legalidad: en el uso, captura, recolección y tratamiento de datos personales, se dará aplicación a los tratados internacionales vigentes y aprobados por Colombia; así como a las demás fuentes del derecho internacional aplicables, a la Constitución, las Leyes Orgánicas, Estatutarias, Ordinarias, Decretos, Ordenanzas, Acuerdos, Reglamentos y Estatutos, así como a las demás disposiciones vigentes y aplicables que rigen el tratamiento de datos personales y demás derechos fundamentales conexos.

Principio de libertad: el uso, captura, recolección y tratamiento de datos personales sólo puede llevarse a cabo con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal, estatutario, o judicial que releve el consentimiento.

Principio de finalidad: el uso, captura, recolección y tratamiento de datos personales a los que tenga acceso y sean acopiados y recogidos por cualquier tercero, estarán subordinados y atenderán una finalidad legítima, la cual debe serle informada al respectivo titular de los datos personales.

Principio de veracidad o calidad: la información sujeta a uso, captura, recolección y tratamiento de datos personales debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de transparencia: en el uso, captura, recolección y tratamiento de datos personales debe garantizarse el derecho del Titular a obtener ante el encargado o ante el responsable del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de cualquier tipo de información o dato personal que sea de su interés o titularidad.

Principio de acceso y circulación restringida: los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados.

Principio de seguridad: Los datos personales e información usada, capturada, recolectada y sujeta a tratamiento, será objeto de protección en la medida en que los recursos técnicos y estándares mínimos así lo permitan, a través de la adopción de medidas tecnológicas de protección, protocolos, y todo tipo de medidas administrativas que sean necesarias para otorgar seguridad a los registros y repositorios electrónicos evitando su adulteración, modificación, pérdida, consulta, y en general en contra de cualquier uso o acceso no autorizado.

LA JURISPRUDENCIA COMO VERDADERA FUENTE DEL DERECHO DE *HABEAS DATA* EN COLOMBIA

Así mismo la ingente Jurisprudencia y un sin número de pronunciamientos que ascienden a más de dos centenares, dados en la mayoría de las veces dentro de las denominadas «Acciones de Tutela «emitidos en instancia de revisión por nuestra Corte Constitucional desde 1992 y hasta la fecha han marcado el derrotero y fijado una suerte de precedentes jurisprudenciales de gran valía que son referente no solo en Colombia, sino incluso allende las fronteras. La primera Sentencia de la que tenemos noticia fue la emitida dentro de una acción de Tutela y su nomenclatura es: T 414 de 1992. A continuación, así como en el apartado de bibliografía, referenciaremos de manera detalle una muestra de la jurisprudencia existente más relevante.

De acuerdo con lo reseñado en el Observatorio sobre datos personales en Colombia Ciro Angarita Barón, podemos destacar por su importancia y relevancia, las siguientes sentencias y pronunciamientos judiciales:

Sentencia T-414 de 1992

a) La dignidad humana, supremo principio de la Constitución de 1991.; b) Las nuevas tecnologías y la libertad personal.; c) Intimidad y *habeas data:* aproximación al artículo 15 de la Carta; d) Intimidad y derecho a la información; e) El Dato y su «propiedad»; f) Los bancos de datos y el derecho constitucional informático; g) Caducidad del dato personal: La cárcel del alma y el derecho al olvido; h) Creciente informatización social e insuficiente protección jurídica; i) Uso responsable de la Informática

Sentencia SU-082 de 1995

a) ¿La manera como una persona atienda sus obligaciones económicas para con las instituciones de crédito, pertenece al ámbito de su intimidad?; b) Derecho al buen nombre y a la información; c) El *habeas data:* su contenido y los medios jurídicos para su protección; d) El conflicto entre el derecho a la información y el derecho al buen nombre; e) Los datos personales y las diversas clasificaciones de la información. f) Límite temporal de la información: la caducidad de los datos.

Sentencia T-729 de 2002

a) El contenido y alcance del derecho constitucional al *habeas data* o a la autodeterminación informática; b) Principios de la administración de datos personales.

Sentencia C-1011 de 2008

a) Explicación y precisiones sobre la ley 1266 de 2008, la cual regula el dato comercial y financiero entendido como aquel relacionado con las obligaciones dinerarias *(Habeas data* financiero); y b) Principios para la administración de datos personales.

Sentencia C-334 de 2010

a) Información genética y autodeterminación informática, y b) Datos personales públicos, privados, semiprivados y reservados.

Sentencia C-748 de 2011

Todos los aspectos de la ley 1581 del 17 de octubre de 2012 »por la cual se dictan disposiciones generales para la protección de datos personales».

Sentencia SU 458 de 2012

Bases de datos relacionados con antecedentes penales; dato personal sobre antecedentes personales; Principios de finalidad, utilidad, necesidad, y circulación restringida.

Sentencia T-987 de 2012

Registros de información exclusivamente desfavorables («listas negras» /»blacklisting«); lista de viajeros no conformes; principios del *habeas data* como límite al tratamiento de datos personales; prácticas abusivas en la administración de datos personales; transporte aéreo como servicio público esencial; principio de acceso equitativo a los servicios públicos.

Sentencia de feb. de 2013 del Consejo de Estado

¿Se vulneran los derechos fundamentales del accionante, por el hecho de que aún persistan respecto del mismo anotaciones de carácter sancionatorio relacionadas con una condena que ya cumplió, en la base datos que administra la Procuraduría General de la Nación?; Registro de sanciones por parte de la Procuraduría General de la Nación.

Sentencia T-643 de 2013

¿Vulnera una persona los derechos a la propia imagen, la intimidad, el buen nombre y la honra de otra, cuando se niega a retirar las imágenes de esta última de un sitio web abierto al público y de otros medios de publicidad sobre los que tiene control, cuando (i) las imágenes fueron tomadas y divulgadas con base en una autorización general para ser usadas con fines publicitarios no específicos; (ii) quien aparece en ellas nunca consintió expresamente en que fueran divulgadas en un contexto en el cual aparece proyectada en un rol que puede ser asociado a la prestación de servicios sexuales; y (iii) esto ha tenido efectos negativos en su vida familiar y social?

NORMATIVA Y DISPOSICIONES LEGALES Y REGLAMENTARIAS APLICABLES

Pasaron varios años desde la expedición de la Constitución de 1991, para que el precepto constitucional, ya mencionado, fuera abordado y desarrollado de manera positiva, por ello hoy podemos afirmar que el derecho fundamental de protección de datos personales – *habeas data,* se encuentra desarrollado y consignado en la Ley estatutaria n.º 1266 de 2008, la cual debe ser aplicada junto con la Sentencia de la Corte Constitucional C – 1011 de 2008 que declaro exequible esta norma con algunas modulaciones que hizo esa alta corporación; y sus Decretos Reglamentarios Decreto 1727 de 2009 y Decreto 2952 de 2010. Vale decir que la Ley 1266 de 2008 brinda protección únicamente a los datos comerciales y financieros, y que por ende no colmaba las expectativas para poder hablar de un grado amplio y completo de protección en Colombia.

Por esa razón se buscó expedir otra ley que cubriera las disposiciones generales sobre datos personales y se extendiera a otros tipos de datos, tales como datos laborales, académicos, de salud, penales, tributarios y sensibles (datos sobre origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos).

Por ello se tramitó otra ley estatutaria, que fue aprobada a finales de 2010, más exactamente el 16 de diciembre de ese año; y como es menester surtió su control constitucional previo ante la Corte Constitucional por tratarse de una Ley estatutaria. La Corte Constitucional emitió la sentencia de constitucionalidad C – 748 de la referida ley el 06 de octubre de 2011, pero, de manera inexplicable, sólo hasta el 25 de julio de 2012 la Corte dio a conocer el texto de la referida sentencia. Fue así como el 17 de octubre el Presidente de la República sancionó y numeró la Ley como la n.º 1581 de 2012. Esta norma estatutaria fue a su turno reglamentada a través del Decreto 1377 de 2013, y del Decreto reglamentario parcial n.º 886 del 13 de mayo de 2014 por medio del cual se reglamenta lo relativo al Registro Nacional de Bases de Datos.

El Decreto 1377 de 2013, fue expedido entonces con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012, y desarrollar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los»derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al

Tratamiento de datos personales, este último tema referido a la rendición de cuentas. El Decreto 1377 de 2013, brindo un periodo de gracia y la oportunidad de «refrendar» el uso de muchos de los datos utilizados hasta ese entonces, pues en su artículo 10 dispuso una especie de «el que calla otorga», buscando una amnistía o formula que permitiera un borrón y cuenta nueva frente a los datos personales recolectados y objeto de tratamiento hasta ese momento, para permitirle a los responsables y encargados de hacer tratamiento de datos personales poder continuar o no, usando los datos capturados hasta ese momento. Se impuso un deber de diligencia y cuidado con un término de tiempo determinado, dentro del cual se debían utilizar y desplegar múltiples canales de comunicación para llegar a los titulares de los datos personales; y repetimos, refrendar o legitimar el poder seguir haciendo uso y tratamiento de los mismos. Veamos:

«Artículo 10. Datos recolectados antes de la expedición del presente decreto. Para los datos recolectados antes de la expedición del presente decreto, se tendrá en cuenta lo siguiente:

1. Los responsables deberán solicitar la autorización de los titulares para continuar con el Tratamiento de sus datos personales del modo previsto en el artículo 7.º anterior, a través de mecanismos eficientes de comunicación, así como poner en conocimiento de estos sus políticas de Tratamiento de la información y el modo de ejercer sus derechos.
2. Para efectos de lo dispuesto en el numeral 1, se considerarán como mecanismos eficientes de comunicación aquellos que el responsable o encargado usan en el curso ordinario de su interacción con los Titulares registrados en sus bases de datos.
3. Si los mecanismos citados en el numeral 1 imponen al responsable una carga desproporcionada o es imposible solicitar a cada Titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información y el modo de ejercer sus derechos, el Responsable podrá implementar mecanismos alternos para los efectos dispuestos en el numeral 1, tales como diarios de amplia circulación nacional, diarios locales o revistas, páginas de Internet del responsable, carteles informativos, entre otros, e informar al respecto a la Superintendencia de Industria y Comercio, dentro de los cinco (5) días siguientes a su implementación. Con el fin de establecer cuándo existe una carga desproporcionada para el responsable se tendrá en cuenta su capacidad económica, el número de titulares, la antigüedad de los datos, el ámbito territorial y sectorial de operación del responsable y el mecanismo alterno do comunicación a utilizar, de manera que el hecho de solicitar el consentimiento a cada uno de los Titulares implique un costo excesivo y que ello comprometa la estabilidad financiera del responsable, la realización de actividades propias de su negocio o la viabilidad de su presupuesto programado. A su vez, se considerará que existe una imposibilidad de solicitar a cada titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información y el modo de ejercer sus derechos cuando el responsable no cuente con datos de contacto de los titulares, ya sea porque los mismos no obran en sus archivos, registros o bases de datos, o bien, porque estos se encuentran desactualizados, incorrectos, incompletos o inexactos.
4. Si en el término de treinta (30) días hábiles, contado a partir de la implementación de cualesquiera de los mecanismos de comunicación descritos en los numerales 1, 2 y 3, el Titular no ha contactado al Responsable o Encargado para solicitar la supresión de sus datos personales en los términos del presente decreto, el responsable y encargado podrán continuar realizando el Tratamiento de los datos contenidos en sus bases de datos para la finalidad o finalidades indicadas en la política de Tratamiento de la información, puesta en conocimiento de los titulares mediante tales mecanismos, sin perjuicio de la

facultad que tiene el Titular de ejercer en cualquier momento su derecho y pedir la eliminación del dato.

5. En todo caso el Responsable y el Encargado deben cumplir con todas las disposiciones aplicables de la Ley 1581 de 2012 y el presente decreto. Así mismo, será necesario que la finalidad o finalidades del Tratamiento vigentes sean iguales, análogas o compatibles con aquella o aquellas para las cuales se recabaron los datos personales inicialmente.

Parágrafo. La implementación de los mecanismos alternos de comunicación previstos en esta norma deberá realizarse a más tardar dentro del mes siguiente de la publicación del presente decreto.»

Como se observa entonces, la expedición de la Ley estatutaria 1581 del 17 de octubre del 2012, y en especial con el contenido y alcance de su Decreto Reglamentario parcial n.º 1377 de 2013, fue menester hacer por una sola vez y en dentro de ese MOMENTO determinado, llegar a los titulares de los datos personales hasta entonces recabados, y hacer un UP DATE, actualización, confirmación y reconfirmación de la autorización y/o refrendación de la misma, para con ello permitirle y darle una nueva oportunidad al titular del dato, para conocer quién y qué clase de datos se tenían de Él por terceros; dándole, repetimos una nueva oportunidad para expresar, otorgar, negar o restringir, de manera libre, previa, expresa, voluntaria, y debidamente informada, a quienes hagan tratamiento de sus datos, recolectar, recaudar, almacenar, usar, circular, suprimir, procesar, compilar, intercambiar, dar tratamiento, actualizar y disponer de los datos que han sido suministrados desde el momento en que sus datos han sido involucrados en las distintas bases o bancos de datos, así como repositorios electrónicos dispuestos para tales efectos.

En el momento en que el titular del dato personal se enteraba y recibía la notificación respectiva a través de cualquier mecanismo idóneo y efectivo; el responsable o encargado de haber hecho tratamiento anterior, quedaba legitimado o autorizado de manera inequívoca para mantener y manejar toda su información; al menos, y es este el punto central, que la persona manifestara de manera directa, expresa y por escrito bien sea en medio físico o electrónico, lo contrario. Una vez el titular del dato personal recibía la notificación, podía entonces, guardar silencio o no responder, con lo cual aceptaba que se continuara haciendo uso de sus datos, o debía manifestar lo contrario de manera directa, expresa, inequívoca y por escrito dentro de los treinta (30) días hábiles contados a partir de la recepción de la referida comunicación a la cuenta de correo electrónico, físico o lugar y forma dispuesto para tal efecto.

En la notificación respectiva que recibía el titular del dato personal, también se le debía informar y dar a conocer la respectiva política de tratamiento de datos personales, las condiciones de privacidad y seguridad en que será tratado su dato personal, su buen manejo, y en especial las condiciones relacionadas con la recolección, uso, almacenamiento, circulación, accesos y demás actividades involucradas para tales efectos.

Nelson Remolina, reconocido tratadista colombiano, en un artículo publicado en el Diario Portafolio, manifestó en ese entonces, y sobre este particular:

«Salvo muy pocas excepciones, la ley obliga a todas las entidades públicas y privadas a revisar qué están haciendo con los datos personales contenidos en sus sistemas de información y replantear varias cosas para ajustarse a la misma. Pero al mismo tiempo, la misma es una oportunidad para que las organizaciones repiensen sobre el uso que se da a esa información y lo actualicen a la luz de las necesidades actuales y futuras.

En otras palabras, todas las entidades tienen dos opciones. Primera: simplemente ajustarse a la ley; Segunda: no sólo cumplir la ley sino renovar sus políticas para dar luz verde a otros usos lícitos que generan valor agregado a sus sistemas de información.

Lo que sí no deben hacer es quedarse dormidos y esperar a que les inicien investigaciones o les impongan sanciones. Datos recientes de la Superintendencia de Industria y Comercio (SIC) muestran que siguen creciendo significativamente las unas y las otras, lo cual pone de presente que varias organizaciones no han adoptado estrategias apropiadas para mitigar los riesgos jurídicos, económicos y reputacionales por infracciones a las reglas sobre protección de datos personales.»

ALGUNAS DEFINICIONES Y TERMINOLOGÍA USUAL EN MATERIA DE DATOS PERSONALES

Tanto para los especialistas, los iniciados, y profanos en el tema de protección de datos personales – *habeas data,* vale la pena mencionar y tener claro algunos conceptos que la normativa vigente en Colombia trae y recoge, en especial el glosario de términos y definiciones que se mencionan tanto en las Leyes estatutarias 1266 de 208 y 1581 de 2012, en particular el Art. 3 de esta última disposición, pero que además el resto de normas nos brindan en el grueso de su articulado; tales como dato privado, semiprivado y público, y definiciones que son de singular importancia para el tema, veamos:

— Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;

— Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;

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

— Encargado del Tratamiento: 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;

— Responsable del Tratamiento: 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;

— Titular: Persona natural cuyos datos personales sean objeto de Tratamiento;

— Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

DATOS SENSIBLES Y SU TRATAMIENTO

Los Artículos 5 y 6 de la Ley 1581 de 2012, contemplan tanto la definición como el tratamiento de los denominados dato sensible. Allí se hace una amplia descripción y se alude por primera vez al dato Biométrico, como por ejemplo la captura de huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc.

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc.

Se podrá hacer uso y tratamiento de los datos catalogados como sensibles cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;

b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización;

c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular;

d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

OBLIGACIÓN Y NECESIDAD DE OBTENER LA AUTORIZACIÓN PREVIA, EXPRESA E INFORMADA DEL TITULAR DE DATOS PERSONALES

Un punto central en la Normativa internacional, y que se retoma por supuesto en la legislación Colombiana, en particular en los artículos 9 y 10 de la Ley 1581 de 2012, es el que tiene que ver con la autorización previa expresa e informada que debe dar u otorgar el titular del dato personal, la cual puede darse por cualquier medio que luego pueda ser objeto de consulta y verificación posterior.

Se tiene entonces, que recolección, almacenamiento, uso, circulación o supresión de datos personales por parte de cualquier tercero, requiere del consentimiento libre, previo, expreso e informado del titular de los mismos. Por ende la autorización previa, expresa e informada, a los que está subordinado el derecho de *habeas data* y la protección de datos personales, se deberán tener en cuenta como premisas la aplicación al derecho a la autodeterminación informática y el principio de libertad. La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales.

La libertad tiene que ver con el hecho de que ésta podría resultar vulnerada al restringirse indebidamente con ocasión de la circulación de datos que no consulten la verdad, o que no haya sido autorizada por la persona concernida o por la ley. El derecho de revocar en cualquier momento la autorización otorgada para el tratamiento de datos personales, surge como consecuencia directa de la autorización previa, expresa e informada que es menester haber logrado en todos los casos.

La legislación vigente establece de manera directa, los casos o eventos donde no se requiere la autorización; y trae como eventos que se pueden realizar sin autorización, cuando se trate de:

— 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.

DERECHOS DE *HABEAS DATA* DE LOS NIÑOS, NIÑAS Y ADOLESCENTES

La regla general establece que queda prohibido el Tratamiento de datos personales de niños, niñas y adolescentes, y que se le dará un trato prevalente, preferente y privilegiado, salvo aquellos datos que sean de naturaleza pública. Por lo tanto se convierte en una constante y un deber del Estado, proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Sobre este particular, resulta de gran importancia mencionar el denominado Memorando de Montevideo la protección de las niñas, niños y adolescentes en Internet y las redes sociales digitales. Conductas como la pornografía infantil, pedofilia, el turismo y acoso sexual a menores *(Grooming* y el *ciberbullying),* deben ser neutralizados y combatidos en la red mundial de información.

El Memorandun de Montevideo como un instrumento internacional de norma de conducta o recomendación que se deben implementar por los Países, la sociedad y comunidad, y todos los involucrados en este tema; para adoptar una serie de postulados los cuales fueron acordados en un seminario de trabajo realizado en la capital Uruguaya, Montevideo los días 27 y 28 de julio de 2009. Un insumo muy valioso de dicho texto fue el trabajo en equipo y el aporte intelectual de muchos académicos, profesionales y expertos de varios países latinoamericanos (Méjico, Ecuador, Argentina, Colombia, Brasil, Perú y Uruguay), Canadá y España.

JURISPRUDENCIA EMITIDA POR LA DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE COLOMBIA

En un pronunciamiento emitido el veintitrés (23) de enero del año Dos Mil Catorce (2014), y que recoge muchos de los postulados y precedentes dados en reiterada jurisprudencia Colombina, la Superintendencia de Industria y Comercio (SIC), Delegatura para la protección de datos personales, en ejercicio de las facultades jurisdiccionales que le otorgo el código general del proceso, le solicito a la relatoría de la sala penal de la Corte Suprema de Justicia suprimir datos de menores de edad en versiones públicas de las sentencias.

El caso se dio cuando se publicó en el sitio Web de la alta corporación judicial una sentencia donde aparecieron de manera evidente, clara e identificable los datos personales que permitían identificar a una menor de edad víctima de abuso sexual. Esta situación, y la subsiguiente publicación del nombre de la menor, sin la debida anonimización, provocó que la niña fuera víctima de matoneo *(bullying)* escolar. Lo anterior como es claro ponía en entre dicho y afectaba de manera palmaria la especial protección otorgada a los niños por la normativa vigente en Colombia sobre Protección de Datos Personales — *Habeas Data.*

En esta oportunidad la SIC, aprovecho para reiterar la necesidad de brindar especial protección a los denominados datos personales sensibles, que afecten la intimidad o puedan generar discriminación, especialmente cuando exista un riesgo de vulneración de los derechos fundamentales de los menores de edad. La disponibilidad de los datos personales de los menores

de edad en decisiones judiciales que se publican en internet, tiene la potencialidad de generar conductas discriminatorias en su contra y por eso es procedente la adopción de medidas que permitan proteger su dignidad, agrega la SIC.

La decisión de la Delegatura para la Protección de Datos Personales de la SIC se adoptó como consecuencia de la denuncia interpuesta por la familia de la menor donde se puso de presente que la publicación de sus datos, y su fácil acceso por internet, había producido incidentes de matoneo escolar en contra de la menor. La Superintendencia le recordó a la Relatoría de la Sala Penal de la Corte Suprema de Justicia, el carácter sensible que tiene la información de los menores de edad y la especial protección que a dichos datos les dio la Ley 1581 de 2012 (Ley General de Protección de Datos Personales).

La SIC también le puso de presente a la Relatoría de la Sala Penal de la Corte Suprema de Justicia, el carácter especialmente protegido de la información sensible que pueda generar discriminación en contra de su titular, tal y como sucede con los datos que identifican a un menor de edad víctima de un delito.

Este pronunciamiento y prohibición de la SIC., se hizo extensiva la orden también fue impartida a la sociedad V Publicaciones S.A.S. – representantes en Colombia de la editora española de contenidos jurídicos, VLEX NETWORKS, S.L. que publicó la sentencia en su sitio web.

APLICACIÓN DE LAS REGLAS DE HEREDIA

En el anterior pronunciamiento, la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio (SIC), dio cabal cumplimiento a las denominadas reglas de Heredia, adoptadas en el año 2003 aprobadas durante el Seminario Internet y Sistema Judicial realizado en la ciudad de Heredia (Costa Rica), los días 8 y 9 de julio de 2003 con la participación de poderes judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay. Las reglas de Heredia, son entonces y fueron aprobadas como unas reglas mínimas para la difusión de pronunciamientos judiciales en Internet, y que se constituyen en últimas en unas recomendaciones y normas tipo, las cuales fueron adoptadas en la ciudad de Heredia, en Costa Rica y que plantean reglas claras sobre este tema cuando de providencias judiciales se trata.

TRANSFERENCIA DE DATOS A TERCEROS PAÍSES. UTILIZACIÓN Y TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES E INFORMACIÓN PERSONAL

Este es otro de los eventos, donde la legislación Colombiana prohíbe de manera expresa la transferencia de datos personales de cualquier tipo a terceros países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la autoridad nacional de protección de datos, para el caso Colombiano, la Delegatura de protección de datos personales de la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la normativa nacional de nuestro País exige a sus destinatarios.

Sin embargo esta regla general, que a primera vista parece tan estricta, y que estable la prohibición de transferir datos personales a otros países no regirá cuando se trate de:

— Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;

— Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;

— Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;

— Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;

— Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;

— Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción en el presente artículo, corresponderá a la Delegatura de Protección de Datos Personales Colombina, Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

REGISTRO NACIONAL DE BASES DE DATOS

El Registro Nacional de Bases de Datos (RNBD) está regulado en el Art. 25 de la ley 1581 de 2012, y fue desarrollado o reglamentado a través del Decreto 886 de mayo de 2014. El RNBD, es en palabras sencillas, un directorio público de las bases de datos sujetas a Tratamiento que operan en el país. Este registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.

Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la legislación vigente.

DECRETO 886 DEL 13 DE MAYO DE 2014

El 13 de mayo de 2014, se dieron dos eventos importantes en lo que respecta al tema de Protección de Datos Personales-Data Protection-*Habeas Data*. El primero a nivel internacional cuando Google sufre otro revés, y el Tribunal de Justicia de la Unión Europea (TJUE), ratifica y respalda, mediante Sentencia, la tesis que ha venido sosteniendo de tiempo atrás en contra del buscador y motores de búsqueda, la Agencia Española de Protección de Datos (AEPD), donde se trató el tema del denominado DERECHO AL OLVIDO, tras una acción iniciada por el ciudadano Español Mario Costeja González.

El segundo a nivel local, cuando el Gobierno Colombiano expide el Decreto reglamentario n.º 886 del 13 de mayo de 2014 a través del cual se entra a regular lo atinente al Registro Nacional de Bases de Datos (RNBD) tanto manuales como automatizadas, mencionado en el Art. 25 de la Ley 1581 de 2012, estableciéndolo como un directorio público de las bases de datos personales, sujetas a tratamiento que operen en el territorio nacional y que será administrado por la Superintendencia de Industria y Comercio; y lo más importante, que estará al alcance del todos los ciudadanos.

La primera pregunta que surge, es por supuesto, desde cuándo empieza a operar el mencionado registro, en qué condiciones y términos y cuáles son los elementos e información mínima que debe contener este registro. Por lo pronto, podemos manifestar, que conforme al Art. 12 del Decreto 886 del 13 de mayo de 2014, por el cual se reglamenta el RNBD, se tiene que todos los Responsables del Tratamiento de datos personales, deberán inscribir todas sus bases de datos existentes dentro del año siguiente, contado, no a partir del presente Decreto, sino contado a partir del momento en que la Superintendencia de Industria y Comercio (SIC), habilite el registro nacional de bases de datos; y de acuerdo con las instrucciones adicionales que para el efecto imparta la SIC.

Una vez y luego, de que este habilitado y funcionando el registro nacional de bases de datos (RNBD), cada base de datos que se creen con posterioridad a ese plazo, deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

Otro punto importante, es el que establece el Art. 3 del Decreto, pues será un deber de los responsables del tratamiento de datos personales, inscribir de manera independiente en el RNBD, cada base de datos que se tenga, y que contengan datos personales sujetos a Tratamiento. Aquí, destacamos otro punto importante que deberá tenerse presente no solo por los obligados inscribirse, sino por la misma SIC; pues entendemos la necesidad de registro independiente de todas y cada una de las bases de datos, pero será necesario que no se caiga en duplicación de la información y los datos personales registrados. Lo anterior sin perjuicio de los principios generales y específicos aplicables en la recolección, manejo, uso, tratamiento, almacenamiento e intercambio, de datos personales.

La finalidad del RNBD, como la de todo registro público, será la de brindar publicidad y oponibilidad frente a terceros sobre la existencia de bases de datos de carácter personal y servirá como herramienta de supervisión por parte de los titulares de datos personales. La Corte Constitucional en sentencia C-748 de 2011, al declarar la exequibilidad condicionada del Art. 25 de la Ley 1581 de 2012, y al referirse a la finalidad del RNBD preciso que «debe permitir a cualquier persona determinar quién está haciendo tratamiento de sus datos personales para de esa forma garantizar que la persona pueda tener control efectivo sobre sus datos personales al poder conocer clara y certeramente en qué bases se manejan sus datos personales». Esta es una finalidad que se vuelve una constante en todos los registros similares llevados en otras latitudes.

De igual forma, la SIC, tal y como lo ordeno la Corte Constitucional en la sentencia ya referida, deberá tomar como base para habilitar el RNBD, los estándares internacionales; y agregaríamos nosotros que también a las normas técnicas existentes para garantizar lo relativo a la seguridad de la información como un requisito para el registro de la información y los datos. Así por ejemplo, sugerimos tener en cuenta las norma ISO 9000 y 15489 sobre gestión documental, y las normas ISO 27001 y 27002 sobre seguridad de la información, así como tener presentes las normas de conducta, protocolos y procedimientos que usualmente recomienda la Unidad de Delitos Informáticos de la Fiscalía General, o en el manual de uso de servicios informáticos, o en las políticas de uso de TIC´s establecidas al interior de cada organización o entidad. Para ello será de gran utilidad tener presente lo dispuesto en el literal H) del Art.) 21 de la ley estatutaria 1581 de 2012, y el Art. 26 del Decreto 1377 de 2013. No estaría de más que la SIC., expidiera las directrices necesarias en lo referente a los lineamientos sobre seguridad. Así mismo, manifiesta el alto tribunal constitucional, que se deberá acudir a las experiencias de otros Estados y Países. Seguramente seguiremos las orientaciones de la Agencia Española de Protección de Datos y lo establecido en la Directiva Europea sobre protección de datos personales.

Es importante resaltar la destacada labor que sobre la tutela y protección de los datos personales de los ciudadanos viene realizando la Delegatura de Protección de Datos Personales

de la Superintendencia de Industria y Comercio, no solo en el desarrollo, divulgación y en particular como autoridad de control y sancionatoria en estos temas. Sobre este particular son ingentes las sanciones que ha impuesto la SIC, a los responsables y encargados de los datos personales.

SANCIONES Y ASPECTOS PENALES RELACIONADOS CON EL TEMA DE PROTECCIÓN DE DATOS PERSONALES Y *HABEAS DATA* EN COLOMBIA

Mediante la Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, 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, entre otras disposiciones; y que es conocida en Colombia como la Ley de delitos informáticos, se establece como bien jurídico tutelado, precisamente la información y los datos; se establecieron de manera positiva y fueron tipificados como delitos – hecho punibles, algunos tipos penales que sancionan, entre otros, ciertos aspectos relacionados con el tratamiento de datos personales como el acceso no autorizado a sistemas de información, la destrucción o manipulación de datos, la suplantación de sitios web para capturar datos personales y la violación de datos personales. Este tipo penal entra a sancionar con prisión de 4 a 8 años y multa de 100 a 1000 salarios mínimos legales mensuales. Veamos:

«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.»

En otras palabras, se fijan los diversos eventos y conductas que generan responsabilidad penal tratándose del tratamiento de datos personales. El deber de diligencia y cuidado de los responsables, como los encargados del tratamiento de datos personales, deberán desplegar una serie de gestiones y tomar medidas efectivas, para poder evitar incurrir en responsabilidad penal. Se establece un agravante al tipo penal cuando la pena señalada se aumenta de la mitad a las tres cuartas partes si la conducta la cometiere el responsable de la administración, manejo o control de dicha información. A lo anterior se agrega el hecho de que si el infractor se puede hacer acreedor a una pena de prisión de hasta por tres años, y la pena accesoria de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Sobre este particular, resultan altamente importantes e interesante, las consideraciones que se reseñan en el Sitio Web del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática (GECTI), de la Facultad de Derecho de la Universidad de los Andes de Colombia, se reseña de manera precisa, más precisamente en el Sitio Web del observatorio Ciro Angarita Barón sobre protección de datos personales en Colombia, en un interesante artículo realizado por Nelson Remolina Angarita en 2013/04/18, veamos:

«Según datos estadísticos del INPEC (Instituto Nacional Penitenciario y Carcelario) 41 personas han sido condenadas por el delito de violación de datos personales. De otra parte, desde el 1 de marzo de 2010 hasta el 22 de marzo de 2013, la Superintendencia de Industria y Comercio (SIC) ha impuesto 544 multas por $4.719.129,675 (US$2.556,408).

Las sanciones de la SIC se refieren a situaciones de infracciones de la ley de *habeas data* financiero (Ley 1266 de 2008). Los principales motivos de las mismas son: (1) No veracidad de la información reportada; (2) Falta de atención debida de reclamos y peticiones de los titulares

de los datos; (3) Omisión de la comunicación previa a la persona antes de reportarla a las centrales de riesgo y (4) recolección de datos sin autorización del titular.

La información sobre las condenas penales fue publicada por el INPEC el pasado 5 de abril de 2013 en las estadísticas tituladas: Modalidades delictivas población internos marzo de 2013.»

PROYECTO DE LEY 2014, MODIFICATORIO LEY 1266 DE 2008

En la actualidad, al momento en que escribíamos este artículo y realizábamos este trabajo, en el Congreso Colombiano a través de los senadores liberales Jaime Durán Barrera y Luis Fernando Velasco, acaban de radicar en la Secretaría General de la Cámara, el proyecto de ley 090 de 2014 Cámara, «Por medio del cual se modifica y adiciona la Ley Estatutaria 1266 de 2008, y se dictan disposiciones generales del *Habeas Data* con relación a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países». Según los autores, la propuesta busca un mayor blindaje a la información financiera, crediticia y comercial de los colombianos.

Dentro de los aspectos fundamentales que contempla el proyecto de ley estatutaria se destacan:

— El tiempo de permanencia del reporte negativo en las centrales de riesgo, corresponderá al mismo de la mora, máximo dos años.

— El tiempo que dura el reporte negativo en las centrales de riesgo, cuando no se ha pagado la deuda será máximo de cinco años.

— Cuando el reporte negativo sea por suma hasta a un (1) salario mínimo legal mensual vigente, con el pago se eliminará de inmediato.

— Cuando una persona está en mora, su calificación disminuye y aunque pague esta no sube, se normaliza de inmediato.

— El tiempo para reportar a una persona luego de entrar en mora en sus deudas, será de máximo dos (2) años.

— Consultar la información crediticia de los ciudadanos sin importar las veces que se haga, no bajará la calificación financiera.

— No cumplir con la notificación (20) días antes de reportar al deudor, será causal para el retiro del reporte negativo.

— Se establece un nuevo periodo de gracia en donde los ciudadanos recibirán beneficios por pagar sus deudas atrasadas.

2.5 COSTA RICA

Constitución de Costa Rica

Artículo 23: El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley.

NORMATIVA COSTARRICENSE SOBRE PROTECCIÓN DE DATOS

La Ley 8968, Ley de protección de la persona frente al tratamiento de sus datos personales, es reciente en el país, en comparación con otras legislaciones. El 5 de septiembre del 2011, se

crea mediante ley la Agencia de Protección de Datos de los Habitantes (Prodhab), adscrita al Ministerio de Justicia y Gracia de Costa Rica.

En esta era digital que vivimos hoy en día, con los avances tecnológicos y la migración de la operatividad de las empresas al ecosistema virtual, todos tenemos que interactuar con el internet. Esa interacción, la mayor parte de las veces surge de acreditar nuestra identidad en la internet a fin que sea reconocida por quienes queremos transmitir un mensaje; sea un pariente que deseamos enviar un email, una transacción bancaria, una reserva de cita médica o una consulta de nuestros datos en un website[45] de alguna institución pública.

Ahora, imaginemos por un momento que todos esos datos están siendo usados de manera inadecuada por alguien más. Seguro la idea no te gusta, ¿verdad? Es por ello que la ley de protección de datos trata de asegurar que tus datos personales que andan en poder de terceros no tengan un uso inadecuado y arbitrario.

Todos los ciudadanos tienen un derecho constitucionales de saber el ¿por qué? Y la finalidad con la que se guardan sus datos personales y asimismo cual dependencia del estado es la encargada de tutelar estos derechos —derechos de la personalidad, derecho a la intimidad y el derecho a la autodeterminación informativa— los cuales estudiaremos más delante de manera pormenorizada.

Por ser la Prodhab, un ente muy nuevo dentro de la administración pública, es normal que algunos ciudadanos desconozcan exactamente las funciones que desempeñan con respecto al control del uso de los datos personales del pueblo costarricense. Eso conlleva que no se pueda evaluar la eficacia por parte de los ciudadanos de esta entidad. La mayoría de los ciudadanos desconocen que poseen derechos inherentes a su personalidad, tales como; el derecho a la libertad, el derecho a la autodeterminación informativa, el derecho a la dignidad humana frente a la sociedad tecnológica, la mayoría piensa y cree que el internet es tierra de nadie y con nadie que lo gobierne. Dicho pensamiento no solo es común en Costa Rica, sino en casi todo el istmo centroamericano. En Latinoamérica este tema es muy nuevo, caso contrario al viejo continente donde ya tiene una larga trayectoria en la cultura de la protección de datos personales y la difusión de estos derechos.

Poco se ha escrito del origen de la protección de datos personales en el ámbito costarricense, no obstante existen algunos autores[46] que han hecho referencia al verdadero origen de los mismos, ubicando el nacimiento de la institución en Alemania, pues se le atribuye ser el primer país en salvaguardar los derechos a la intimidad de sus habitantes por medio de mecanismos legales que permiten evitar prácticas abusivas y arbitrarias en el tema. En 1970, el Parlamento de Estado alemán de Hesse, fue el primero en promulgar su normativa de protección de datos denominado «Datenshutz».

Consecutivamente, la iniciativa llegó hasta el parlamento federal de Alemania donde en el 1977 se creó un Comisario Federal para que interviniera en las situaciones donde se percibiera una lesión a los derechos ligados a la intimidad de las personas. Posteriormente, la Unión Europea (UE), a través del Consejo Europeo, redactó en 1995 un instrumento jurídico —denominado Directiva 95/46 CE— vinculante para los países de la UE, donde sí algún país de otro continente deseaba comercializar información sobre datos personales debía cumplir con lo requerido en el documento.

---

45 Anglicismo que significa sitio web.

46 «El reto de Costa Rica frente a la institucionalización de la Agencia de Protección de Datos de los Habitantes, PRODHAB, con fundamento legal en la Ley n.º 8968». Adriana M. RODRÍGUEZ MENDOZA. *Revista Electrónica de la Facultad de Derecho,* ULACIT-Costa Rica. Derecho en Sociedad n.º 3, 2012. Página 130.

Su finalidad fue tan extensiva que se incorporó a los tratados internacionales entre los países de otros continentes. En dicho texto se redactaron algunos de los principios y términos que rigen hoy en día, tales como la calidad de datos, la legitimación del tratamiento, las categorías especiales de tratamiento, información a los afectados por dicho tratamiento, el derecho de acceso del interesado, y el derecho del interesado por oponerse. Estos son aplicables a los datos tratados o no por medios automatizados, de conformidad al Convenio 108, Convenio de la Protección de los Individuos con respecto del procesamiento automático de datos personales.

La ONU, como una entidad de acción mundial abordó el tema de protección de datos, y Costa Rica adoptó algunos de los criterios emitidos para los Estados miembros, por medio de la directriz «Principios rectores para la reglamentación de los ficheros computarizados de datos personales», emitida el 14 de diciembre de 1990, la que tenía como fin servir de guía legal para los demás estados miembros, acá se pactaban parámetros de seguridad jurídica para la manipulación de información personal de las personas naturales y jurídicas.

Estos criterios adoptados por Costa Rica fueron «tropicalizados» al contexto nacional con la finalidad de poder obtener una respuesta más contundente para los ciudadanos costarricenses.

En referencia a los principios que guardan similitud en ambos instrumentos jurídicos, se ha escrito en la doctrina costarricense[47] al decir:

«… por conceptualizarlo de alguna manera, desde una misma interpretación, son los que describe la Ley en la sección I, artículos 4 al 8. Al analizar los principios rectores para la reglamentación de los ficheros computarizados, observamos que el primer principio de la licitud y lealtad, invocado en la directriz de la ONU, se refiere a la prohibición de recopilar los datos personales a través de procedimientos desleales. Al compararlo con lo dispuesto en la normativa costarricense referente al tratamiento de los datos personales, encontramos la adopción de este principio internacional de licitud y lealtad, en el artículo 6, inciso 4, donde se refiere al principio de la calidad de la información, con respecto a la adecuación, el cual dispone que «los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos (…)». El segundo principio sugerido en la directriz es el principio de exactitud, el cual obliga a las personas creadoras de las bases de datos, por verificar que la información custodiada sea exacta; este principio está ligado también al artículo 6, inciso 3, bajo el mismo nombre, sobre la calidad de la información, y exactitud, «… los datos de carácter personal deberán ser exactos (…).

El tercer principio corresponde a principio de finalidad, el cual establece que la creación y utilización de un fichero debe ser especificado y justificado, y se encuentra ligado al capítulo II, artículo 6 inciso 4, sobre adecuación: «… las bases de datos no pueden tener finalidades contrarias a la ley (…)». Otro principio se refiere al principio de acceso de la persona interesada, ya que toda persona tiene derecho a conocer la información que sobre ella administren los ficheros; en Costa Rica lo regula expresamente el artículo 7, sobre los derechos que le asisten a la persona, donde se señala que «se garantiza el derecho a toda persona al acceso de sus datos personales. El principio sobre seguridad, señala que se deben adoptar medidas apropiadas para proteger los ficheros, lo tutela la ley costarricense en la sección III, artículo 10, sobre seguridad de los datos: «El responsable de los bases de datos deberá de adoptar las medidas necesarias para garantizar la seguridad de los datos.

Según el principio de la ONU sobre control y sanciones, cada legislación debería designar a la autoridad, de conformidad con su sistema jurídico, para controlar y fiscalizar el respeto de los principios anteriormente enunciados. En la ley costarricense se ubica en el capítulo V,

---

47 El reto de Costa Rica frente a la institucionalización de la Agencia de Protección de Datos… Páginas 133 y sgts.

sección II, artículo 28, el cual describe tres tipos de categorías: faltas leves, faltas graves y faltas gravísimas para diferentes circunstancias. El otro principio de la directriz se refiere al campo de aplicación, y sugiere que se aplique a todos los ficheros automatizados, tanto públicos como privados. Al igual que en nuestra legislación, lo describe en el capítulo I, artículo 2, sobre el ámbito de aplicación: «Esta ley será de aplicación sobre organismos públicos o privados».

Por último, se encuentra el principio de flujo de datos a través de las fronteras, cuando no haya garantías comparables de protección de vida no se podrán imponer limitaciones injustificadas a la circulación de información fuera de las fronteras de un país. En nuestra ley existe este vacío para regular el flujo de datos a través de las fronteras.

Como se observa en el comparativo anterior, de los principios rectores recomendados por la ONU de aplicación para los Estados miembros, Costa Rica introdujo la mayoría en la normativa que rige la tutela del tratamiento de datos personales, lo cual es evidencia de que sirvió de inspiración para la redacción del marco jurídico que nos rige».

La Organización de Estados Americanos (OEA), donde igualmente Costa Rica es parte, creó el «Proyecto de Convención Americana sobre Autodeterminación Informativa», cuyo fin es reforzar la normativa sobre tratamiento de datos personales de los Estados miembros. Fue promulgado en el 2011 bajo el código CP/CAJP-2921/10 rev.1.

Acá se plasma la moción de regulación para la protección y movimiento internacional de datos, además de abordar temas propios de la materia como el derecho a la información en la recolección de datos, el consentimiento del titular, la calidad, categorías, seguridad y cesión de datos, los derechos y las garantías de las personas, el *habeas data,* las sanciones, los recursos, las agencias de protección de datos y el registro de datos, entre otros.

En virtud de los compromisos adquiridos por la nación costarricense como miembro de las organizaciones mencionadas, es que se introduce en el seno de la asamblea nacional el proyecto de ley sobre la tutela legal del tratamiento de datos personales en Costa Rica. Uno de las principales causas de alargamiento que se dieron en la asamblea nacional en la aprobación del proyecto de ley, fue que el texto de la normativa presentaba ambigüedades —según explican algunos diputados— en los conceptos y los efectos que se perseguía con la normativa. En el proceso se cambiaron algunos conceptos contemplados en el dictamen de la comisión, como por ejemplo el término «dato de carácter personal» por «dato de carácter sensible», para no crear un desequilibrio entre el derecho a la información y el acceso al dato público.

Los antecedentes sobre regulación en el manejo de datos personales de los habitantes en Costa Rica, ha tenido antecedentes legislativos infructuosos, por mencionar tenemos: en 1996, se presentó un proyecto de ley con el fin de incluir vía reforma a la Jurisdicción Constitucional el *habeas data.* Este contó con la aprobación en el primer debate de la asamblea, al momento que se envío a la Sala Constitucional de la Corte Suprema, se determinó la existencia de vicios en el expediente legislativo, lo que la mandó al «cajón del olvido». La Sala argumenta que los derechos que se pretendían tutelar no estaban conceptualizados en el proyecto de ley, también que la ley no regulaba ninguna coerción para quien violara los derechos tutelados, adquiriendo el significado de «letra muerta».

Posteriormente, se trabajó más a fondo sobre la figura del *habeas data,* definiéndolo como un instrumento o mecanismo de garantía procesal a favor de las personas que han sufrido un menoscabo en su ámbito de intimidad producto de usos abusivos de sus datos e informaciones. Así fue que se encuentra asidero para justificar ulteriormente un instrumento jurídico destinado a la prevención de los delitos contra la intimidad. Este primer proyecto abarcaba un recurso de amparo más amplio, con el propósito de tutelar la libertad informática[48].

---

[48] La libertad informática, es considerada por la doctrina española, como un nuevo derecho fundamental que tiene como propósito garantizar la facultad de los individuos para: «conocer y acceder a las informaciones que les conciernen archivados en bancos de datos, (lo que se denominaba *Habeas Data,*

Uno de los principales debates era sobre a que ministerio debía estar adscrito la Prodhab. Primeramente, se le asignó a la Defensoría de los Habitantes[49], pero en el periodo de consultas de la ley, esta dijo que: «Por control de legalidad no podía ser juez y parte en la intervención y defensa de los derechos que tutela la Prodhab.[50]» Este criterio fue considerado por la Asamblea y se redactó la adscripción de la Prodhab al Ministerio de Justicia y Gracia.

Antes de una ley específica en materia de protección de datos, existían artículos dispersos en la normativa vigente sobre este particular, por ejemplo; el código penal, código civil, constitución política, ley general de aduanas, ley de administración financiera de la república y presupuestos públicos, código de normas y procedimientos tributarios y la ley general de telecomunicaciones, entre otras.

El Código Penal (arto 196 bis), sanciona con pena de cárcel de 1 a 3 años, para quienes vulneren la intimidad de otra persona, es decir, que sin su consentimiento se apodere, acceda, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino mensajes, datos e imágenes contenidas en medios electrónicos, informáticos, magnéticos y telemáticos. No obstante no ha tenido la efectividad debida para enfrentar la manipulación de la información por parte de la empresa privada con fines comerciales, casos especifico de los teletrabajos; como oferta de productos financieros, seguros, cobros, etc.

La Ley General de Telecomunicaciones, de manera similar regula el uso de correos, emails, sms y llamadas para ofertar productos. El art. 42 de la referida ley, 8642 dice:

«Los operadores de redes públicas y proveedores de servicios de telecomunicaciones disponibles al público, deberán garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos de carácter personal de los abonados y usuarios finales, mediante la implementación de los sistemas y las medidas técnicas y administrativas necesarias. Estas medidas de protección serán fijadas reglamentariamente por el Poder Ejecutivo.

Los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. En caso de que el operador conozca un riesgo identificable en la seguridad de la red, deberá informar a la Sutel y a los usuarios finales sobre dicho riesgo.

Los operadores y proveedores deberán garantizar que las comunicaciones y los datos de tráfico asociados a ellas, no serán escuchadas, gravadas, almacenadas, intervenidas ni vigiladas por terceros sin su consentimiento, salvo cuando se cuente con la autorización judicial correspondiente, de conformidad con la ley.»

Es curioso mencionar un caso particular, documentado por un estudio en el tema[51], donde una entidad bancaria fue condenada a pagar la suma de un millón de colones a favor de un afectado, por haber sido violentado su derecho a la intimidad; hecho que fue probado mediante

---

por su función análoga en el ámbito de la libertad de información, a cuanto supuso el tradicional *Habeas Corpus* en lo referente a la libertad personal), controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados y disponer sobre su transmisión» ÁLVAREZ DE BOZO, Miriam, PEÑARANDA QUINTERO, Flor M. y PEÑARANDA QUINTERO, Héctor R., «La Libertad Informática. Derecho Fundamental de la Constitución Venezolana». Publicaciones Universidad del Zulia y Organización Mundial de Derecho e Informática. Maracaibo, 1999. p. 22).

49 La Defensoría de los Habitantes de la República es un órgano contralor que forma parte del Poder Legislativo. El fin de esta institución es el de velar porque la actividad del sector público se ajuste al ordenamiento jurídico y la moral, de forma tal que los derechos e intereses de los habitantes cuenten con una tutela efectiva.

50 El reto de Costa Rica frente a la institucionalización de la Agencia de Protección de Datos… Páginas 138 y sgts.

51 El reto de Costa Rica frente a la institucionalización de la Agencia de Protección de Datos… Páginas 140 y sgts.

la grabación de más de 20 llamadas por parte de la entidad, que interrumpieron su jornada laboral y su vida familiar, entre otras actividades. Esta acción civil resarcitoria fue presentada en el 2009 y fue resuelta en el 2012; de esta manera se sentó un precedente donde se tutela de manera efectiva los derechos fundamentales de la privacidad del individuo frente a conglomerados de empresas de carácter internacional. Las consecuencias de esta sentencia fueron el impulso de presentación de causas similares por parte de afectados y un mayor apego de empresas como estas a la normativa vigente.

En materia de delitos informáticos, Costa Rica en los últimos años ha sido víctima de muchos con trascendencia internacional, donde han sido las empresas que con el ánimo de no perder esa cuota de mercado que les brinda el comercio electrónico, es que han tomado la función del estado en crear una cultura preventiva al respecto. Es normal ver como algunas entidades bancarias han optado por educar a la clientela en medidas de seguridad. El estado no se ha limitado a más que hacer lo que puede con la legislación que se tiene vigente.

El delito informático con carácter propio y naturaleza jurídica independiente no ha sido definido legislativamente de manera completa en el país, pues en algunos casos se trata como una modalidad de algunos tipos penales vigentes; como lo son el fraude, robo, chantaje y malversación de caudales públicos, los cuales se convierten en delitos informáticos cuando su consumación se lleva a cabo mediante instrumentos informáticos. A la fecha de hoy, todavía esta un proyecto de ley, denominado proyecto de ley n.º 17613, que busca reformar el artículo 229 bis del Código Penal y adicionar un nuevo capítulo denominado «Delitos Informáticos», buscando incluir tipos penales propios de este tipo de delitos y fortalecer los ya existentes, como; la violación de comunicaciones electrónicas, fraude informático, la alteración de datos, sabotaje informático, integridad e imagen de una persona, suplantación de identidad, el cual es muy susceptible de cometerse por las facilidades de la internet; violación de datos personales, clonación de páginas electrónicas, uso de virus y estafa informática *(phishing)*, entre otros. Al igual que todo tipo de normativa penal que se piense implementar, no basta con leyes punitivas, sino que es imperativo crear conciencia en la población para que analicen y sepan el tipo de información que brindan en el internet.

La tutela de la información por parte del estado en los medios electrónicos es un reto encomiable, pues es necesario estar actualizándose legislativamente de manera constante, pues las formas de delinquir evolucionan y se adaptan constantemente a los cambios del ecosistema virtual que se ha creado alrededor de la internet. Cabe sumarle que las personas que se dedican a esta actividad, reúnen un perfil muy particular donde lo más delicado es el alto *expertise* que poseen. Por ese grado de complejidad es que ya hoy en día en algunas legislaciones y cuerpos de seguridad se les trata como delitos económicos de alta complejidad, equiparado a los *White Collar Crimes*.

AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES

La Agencia de Protección de Datos de los Habitantes (Prodhab), es la encargada de velar por el cumplimiento de la normativa en materia de protección de datos, tanto para personas físicas como jurídicas y fue creada por la Ley n.º 8968. Dentro de sus funciones esta el velar por el cumplimiento de la normativa en materia de protección de datos, incluyendo:

1. Llevar un registro de las bases de datos reguladas por esta ley. Hace referencia a que toda base de datos que no sea registrada en esta Agencia, se tendrá como irregular y no autorizada para existir, sea el sector público o privado quien la maneje.
2. Imponer las sanciones a quienes infrinjan las normas sobre la protección de datos personales y trasladar al Ministerio Público las que se puedan configurar como delito.

En la ley y su reglamento se establecen los procedimientos por medio de los cuales se procede a la sanción en el fáctico.

3. Promover y contribuir en la redacción de la normativa tendiente a implementar las normas que regulan esta materia. Acá se faculta para que se proceda a formular cualquier proyecto de reforma de la normativa con el fin de alcanzar los objetivos propios de la Agencia, siempre actualizándose a las nuevas tecnologías.
4. Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales. Más que una función, lo considero una obligación, pues dentro de los proyectos esta la de información, asesoría y divulgación de la normativa vigente.

También, podrá acceder a las bases de datos reguladas por la ley, estén o no registradas en la Agencia; con el fin de cumplir la normativa vigente, donde operará de oficio o a solicitud de parte, pudiendo ordenar la supresión, rectificación, adición o restricción en el tráfico de datos personales si no están acordes a los parámetros de la ley. Así mismo debe resolver los reclamos interpuestos ante su fuero, dictar las directrices necesarias.

Esas son muchas de las funciones que permite desarrollar la legislación en el ámbito costarricense sobre protección de datos, no obstante es un tema que todavía podría considerarse en embrión. Falta más que normativa la concientización de la sociedad.

MIRADA DE FUTURO Y RETOS

Entretanto en el viejo continente todavía se discuten una tendencia sobre la normativa vigente que busca empoderar al usuario sobre sus propios datos y reducir los costes empresariales, en Costa Rica todavía está en etapa de digestión para las empresas e indigestión para los más conservadores.

Costa Rica tiene el más alto porcentaje de penetración de internet en la población, seguido de su vecino Panamá y en último lugar su otro vecino del sur, Nicaragua. Las empresas relacionados con servicios de internet se han proliferado exponencialmente, dando mucho atención al ecosistema emprendedor y *startups* en el medio. Por ello, es imperante que se empodere los derechos a la privacidad en línea e impulsar la economía digital costarricense. El progreso tecnológico y la globalización han llegado para adueñarse de las riquezas digitales. Han cambiado la forma de hacer negocios, cambiando las reglas del juego en los que se refiere a las vías de obtención, acceso y utilización de los datos. Por ello, debe ser una tarea de primer orden para el estado poder reforzar la confianza del consumidor online, para poder lograr el despegue exponencial de la innovación de empresas digitales en el país.

Otro tema, que ha cobrado especial auge en otros países y de los cuales Costa Rica, puede encontrar muy pronto la necesidad de proteger a sus nacionales es en el referente al tema del «derecho al olvido» donde recientemente se obligó a Google a cambiar su política de almacenamiento de datos en línea: los usuarios podrán borrar sus datos cuando no existan razones legítimas para conservarlos, esto hará que las personas confíen más en internet, en especial en nuestros días en donde existen muchas plataformas de información, como Facebook, Twitter, LinkedIn, Google+, etc.

Costa Rica, como dijimos anteriormente, todavía esta en etapa de gestación. Existe mucho desconocimiento en torno al tema. Las instituciones públicas lideran la culpabilidad de desprotección de datos, han hecho ventas de la información. La Prodhab se estableció 6 meses después de la publicación de la ley, y el Reglamento pasado el año.

Todavía es normal que los usuarios de telefonía celular reciban sms promocionales en su celular sin haber autorizado ello o que se comercialicen bases de datos tal cual fuera un bien de comercio lícito.

A manera conclusiva, diremos que se esta arando el terreno para el empoderamiento de la Prodhab. Como hemos recalcado es importante la protección de datos personales en la economía digital, en donde la información se encuentra en todos lados y se moviliza rápidamente. El modelo que se sigue en Costa Rica, es inspirado en el modelo español de protección de datos, aunque esté por el momento en *«stand by»*, hasta que la ley tome forma en su ámbito de acción.

2.6 ESPAÑA

Constitución Española

Artículo 18.4: La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

ANTECEDENTES

España cuenta con una con un largo recorrido en materia normativa sobre protección de datos de carácter personal, si se compara con otros países. Recogido este derecho fundamental en el artículo 18.4 de la Constitución Española: «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos» obliga al Estado español a garantizar este derecho de las personas. Igualmente deviene obligado desde la firma y ratificación del Convenio n.º 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Ello motiva que se inicie el trámite legislativo que concluye con la promulgación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal[52], vigente hasta el 14 de enero del 2000, momento en el que es sustituida por la vigente Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal[53].

La escasa vigencia de esta Ley Orgánica viene condicionada por la aprobación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[54], que regula sin diferenciar tratamientos automatizados y no automatizados por lo que la Ley Orgánica se quedaba corta al regular sólo los primeros.

Esto incluso provocó una paradoja, que el reglamento de desarrollo de la LO 5/1992, el derogado Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal[55], lo fuera durante la mayor parte de su vigencia, de desarrollo de la LO 15/1999 más que de la LO 5/1992 en cuyo nombre y desarrollo se aprobó. Este Real Decreto fue derogado por el vigente Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de

---

52 Publicado en BOE de 31 de octubre de 1992.
53 BOE núm. 298 de 14 de diciembre de 1999.
54 Diario Oficial de las Comunidades Europeas n.º L 281 de 23/11/1995.
55 BOE n.º 151, 25-jun-1999.

desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[56]. Téngase en cuenta que algunos artículos de este Real Decreto han sido declarados nulos de pleno derecho por las Sentencias del Tribunal Supremo de la Sala 3.ª de 15 de julio de 2010 y 8 de febrero de 2012 (esta segunda STS trae base de una cuestión prejudicial planteada en el primer proceso por una defectuosa transposición de la Directiva 95/46/CE, tras resolución de la cuestión prejudicial mediante Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011 en los asuntos acumulados C-468/10 y C-469/10.

BIEN JURÍDICO PROTEGIDO: DEFINICIÓN DE DATO DE CARÁCTER PERSONAL

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), lo define en su art. 3 a) como «cualquier información concerniente a personas físicas identificadas o identificables».

De acuerdo con la definición que establece la Directiva 95/46/CE, «se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

También la Directiva 95/46/CE, indica en su considerando 26, que: «... para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado[57]; que los códigos de conducta... pueden constituir un elemento útil para proporcionar indicadores sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado».

La guía legal de de protección de datos de carácter personal del Instituto Nacional de Tecnologías de la Comunicación[58], nos propone a modo ejemplificativo, que serán considerados datos de carácter personal el nombre, los apellidos, la dirección postal e incluso la dirección de correo electrónico, así como el número de teléfono fijo, móvil, la dirección IP con la que se navega por Internet, el ADN, cualquier tipo de imagen de una persona física…, y por su parte la Agencia Española de Protección de Datos ha ido delimitando determinados supuestos en concreto a través de la fundamentación en los diferentes procedimientos que ha conocido o a través de los diferentes Informes Jurídicos que a elaborado y las sentencias de los Tribunales dictadas sobre sus resoluciones[59].

---

56 Publicado en BOE núm. 17 de 19 de enero de 2008.

57 Recientemente el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE ha emitido su Dictamen 05/2014 sobre técnicas de anonimización en el que expone su opinión sobre las principales técnicas existentes en la actualidad, sus puntos fuertes y débiles.
Puede ser consultado en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf.

58 Guía legal protección de datos de carácter personal. INTECO.../AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/AppData/Downloads/guia_lopd.pdf León. Marzo de 2008.

59 Así por poner algunos ejemplos el informe 285/2006 sobre número de teléfono y dato de carácter personal, Informe 425/2006 sobre Matrículas de vehículos y concepto de dato de carácter personal. Informes 0549/2008 y 0078/2009 sobre grabación de llamadas por policía local, INSTRUCCIÓN 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Informe 0437/2010 sobre si el correo electrónico profesional es dato de carácter personal o, en esta misma línea pero aplicado al correo electrónico personal las Sentencias de la Audiencia Nacional, Sección. 1.ª, de 23 de marzo 2006 y de 25 de mayo de 2006 afirmando esta

Delimitado el concepto, debemos indicar que la LOPD será de aplicación a los datos de carácter personal que se encuentren «registrados en soporte físico, que los haga susceptibles de tratamiento[60], y a toda modalidad de uso posterior de estos datos por los sectores público y privado», radicando aquí la gran novedad sobre la normativa anterior ya que se regulan tanto los tratamientos automatizados como los no automatizados, salvo las excepciones contenidas en el artículo 2 de la LOPD, entre las que cabe destacar la conocida como excepción doméstica: «ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o doméstica».

INFORMACIÓN Y CONSENTIMIENTO. OBLIGACIÓN DE TRANSPARENCIA

La legislación española, el art. 5 de LOPD establece que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

También establece que cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

Este principio va íntimamente unido al regulado en el artículo 6 de la Ley 15/1999 sobre la obtención del consentimiento[61], y podríamos decir que es el principio legitimador de todo tratamiento. El consentimiento permite al afectado ejercer el control del uso de sus datos personales, lo que viene denominado como derecho de autodeterminación informativa. Sólo a través de una información transparente es posible obtener un consentimiento válido puesto que la finalidad y usos del tratamiento para los que se pide que se otorgue el consentimiento habilitan el tratamiento.

Esto ha llevado al grupo de trabajo a emitir su Dictamen 3/2013 *on purpose limitation* (limitación de la finalidad). De acuerdo con la nota de prensa emitida el 18/4/2013 coincidiendo con la publicación del Dictamen, el Art 29 WP entiende que se deben fijar límites en el recabo y posterior tratamiento de datos Cuando se proporcionan datos personales a una empresa u otra organización, normalmente se tienen ciertas expectativas acerca de la finalidad para la que sus datos serán utilizados. Hay un valor en honor a estas expectativas que es la preservación de

---

última que «con independencia de que la denominación de la dirección corresponda o no con el nombre y apellido de su titular, país o empresa en la que trabaja, lo cierto es que se puede mediante una operación nada difícil, identificar perfectamente a una persona física, ya que esa dirección de correo electrónico aparecerá vinculada a un dominio concreto, por lo que sólo será necesario consultar al servidor en que se gestione dicho servicio. Es más esta Sala, en un caso como el número del Documento Nacional de Identidad, que en principio no tiene aparente relación externa con el nombre y apellido de su titular, ha entendido que es un dato de carácter personal amparado por la LOPD en la sentencia de 27 de octubre de 2004».

60 El artículo 3 c) los define como «operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».

61 Téngase en cuenta que conforme a reiterada doctrina de la Audiencia Nacional la carga de la prueba de la obtención del consentimiento recae sobre el que trata datos personales.

la confianza y la seguridad jurídica. Por ello, el principio de limitación de la finalidad es una piedra angular de la protección de datos.

No obstante, los datos que ya han sido recogidos pueden ser realmente útiles para otros propósitos, que no estén previstos inicialmente. Por lo tanto, también hay valor en permitir, dentro de límites cuidadosamente equilibrados, un cierto grado de uso adicional. De ello se deriva que los datos de carácter personal deberán ser recogidos para fines determinados, explícitos y legítimos y no podrán o ser tratados posteriormente de manera incompatible con dichos fines.

La Ley Orgánica 15/1999 exige la prestación del consentimiento previo e inequívoco[62] del afectado para el tratamiento de sus datos, pero establece una serie de excepciones, de manera que no es necesario prestar consentimiento:

— Cuando una ley así lo dispone.

— Cuando los datos son recogidos para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.

— Cuando se refieren a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y los datos personales son necesarios para el mantenimiento y cumplimiento de ésta.

— Cuando el tratamiento tenga como finalidad proteger un interés vital del interesado y éste se encuentre física o jurídicamente incapacitado para dar su consentimiento.

Esta excepción es específica para el tratamiento de los datos en la actividad de prestación sanitaria asistencial y el afectado está incapacitado para dar su consentimiento. Se permite el tratamiento de datos personales sin consentimiento del interesado en este caso pues existe una colisión entre el derecho a la vida o a la integridad física y el derecho a la intimidad y a la protección de datos.

En todo caso, la excepción del consentimiento no exime de la obligación de informar en los términos que hemos visto en el punto anterior, relativo al principio de información, ni permite el tratamiento de cualquier dato sino únicamente aquellos que cumplan el principio de calidad (datos adecuados, pertinentes, actualizados y no excesivos).

DATOS ESPECIALMENTE PROTEGIDOS Y OTROS TRATAMIENTOS INVASIVOS

De acuerdo con lo establecido en el apartado 2 del artículo 16 de la CE, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión

---

[62] Que se requiera que el consentimiento sea inequívoco ha planteado muchas cuestiones sobre si caben los consentimientos tácitos y en que supuestos. En esta línea el Informe Jurídico 00/2000 sobre Caracteres del consentimiento definido por la LOPD, Informe Jurídico 93/2008 Formas de obtener el consentimiento mediante web. Consentimientos tácitos, Informe Jurídico 300/2009 Consentimiento otorgado en Internet mediante el click en la pestaña acepto, Dictamen del Grupo de Trabajo del artículo 29 15/2011 sobre la definición del consentimiento, Informe Jurídico 11/2014 sobre consentimiento para uso de cookies no cabiendo un sistema de opt-out, y a nivel jurisprudencial por citar algún caso, la Sentencia de la Audiencia Nacional de 27-04-2006.

y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a los que nos hemos referido, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

DATOS RELATIVOS A LA SALUD

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Además de la LOPD, en lo referente a datos de salud, es imprescindible recurrir a otra legislación, como por ejemplo la Ley 14/1986, de 25 de abril, General de Sanidad, Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica o el Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.

DATOS RELATIVOS A MENORES

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) no hace ninguna referencia específica a la protección de los datos del menor ni establece sobre ello ningún tipo de disposición especial. No obstante, el Real Decreto 1720/2007 que la desarrolla permite el tratamiento de datos personales de mayores de 14 años siempre que estos den su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela (como por ejemplo para contratar). La información que va dirigida a estos menores deberá expresarse en un lenguaje que sea fácilmente comprensible.

Hay que recordar las recomendaciones de la Agencia Española de protección de datos[63] que destaca lo ya establecido en el Real Decreto 1720/2007 al disponer que cuando alguien recoge

---

[63] Derechos de niños y niñas, deberes de los padres y madres. Agencia Española de Protección de datos, Madrid, 2008.

datos de menores no puede solicitar datos de su entorno familiar salvo para dirigirse a los padres y madres y solicitar su autorización cuando sea necesaria. Podrán pedirse datos básicos para entrar en contacto con la familia, en la escuela, la asociación deportiva o escolar etc. Está prohibido utilizar al menor para obtener datos innecesarios sobre el resto de la familia como los ingresos, preferencias de ocio, etc.. En el caso de que se recojan datos de menores de catorce años, en todo caso se requerirá el consentimiento de los padres o tutores.

CESIONES DE DATOS

En su artículo 3 y en concreto el apartado i) la LOPD define como Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado. Con carácter general, la LOPD prohíbe una cesión de datos siempre que no se cumpla una serie de requisitos, que básicamente estable en su artículo 11.

Es preciso matizar, que hay que distinguir lo que se entiende por una cesión de datos de lo que es un acceso a los datos por cuenta de terceros, estando este último concepto regulado en su artículo 12 de la LOPD. Por tal se entiende una autorización para acceder a los datos a una empresa o institución que está prestando un servicio que externaliza, sin que en este caso, se considere este hecho como una cesión de datos.

Con carácter general, tal y como se establece en su artículo 11, los datos personales objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del que recibe la información (cesionario) y del que la comunica (cedente), siempre con el previo consentimiento del interesado.

Por lo tanto, para que una cesión de datos esté amparada por la Ley Orgánica de Protección de Datos debe cumplir dos importantes requisitos que la cesión vaya en la línea de dar cumplimiento a los fines relacionados directamente con las funciones legítimas del cedente y del cesionario y que exista un consentimiento previo del afectado. Además, para que este consentimiento se válido, el afectado debe conocer la finalidad a la que se destinarán los datos cuya comunicación consiente y la actividad que desarrolla el cesionario. De no darse estos requisitos, el consentimiento podría considerarse que es nulo.

En este sentido queremos destacar la Sentencia de la Audiencia Nacional de 18 de mayo de 2006 que, entre otros dispone que: «ya hemos dicho que la resolución de la controversia exige relacionar los hechos con lo preceptuado en el artículo 6.1 de la actual Ley de Protección de Datos (el tratamiento de datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa) y en el artículo 11.1 de la misma, a fin de determinar si puede o no considerarse cumplido tal principio del consentimiento o autodeterminación. Nos hemos referido también al contenido «amplio» que, en la legislación actualmente en vigor se otorga al concepto de cesión de datos personales», para continuar afirmando que: «y asimismo es aplicable al caso lo dispuesto en el número 3 del Artículo 11 que declara que «será nulo el consentimiento para la comunicación de datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretende comunicar».

Teniendo en cuenta que la cláusula establecía como finalidad de la cesión de datos a otras entidades «poder, remitirle publicidad u ofertas de otras entidades comerciales o de servicios que pudieran resultar de su interés; en especial, las referidas a la cultura y el ocio, productos y servicios para el hogar o de uso personal (electrodomésticos, textil, cosmética alimentación etc), automoción, inmobiliarios, aseguradores y financieros», esto lleva a la Audiencia Nacional a entender que: «La amplitud de categorías de bienes y servicios para los que se presta el consentimiento, además (publicidad u oferta de cualquier entidad comercial o de servicios

«que pudieran resultar de su interés») tampoco permite al particular identificar de forma determinada y explícita las finalidades para las que serán tratados sus datos personales, en términos que le permitan prestar un consentimiento inequívoco como el exigido por la LOPD» y que por todo ello cabe entender que: «la indicada leyenda no cumple con las exigencias que la legislación de protección de datos (Art. 6 y 11 de la LOPD) requiere en la prestación del consentimiento, de forma que el consentimiento para su comunicación a terceros sea inequívoco por haber facilitado previamente una información expresa, precisa e inequívoca (conforme al artículo 5 de la LOPD), sobre las finalidades determinadas y explícitas para las que se trataron los datos (según el Art. 4.1). El consentimiento resulta, por tanto, nulo, de conformidad con el Art. 11.3 de la LOPD».

No obstante todo lo dicho en los párrafos anteriores, existen una serie de supuestos, en los cuales, no son aplicables las normas generales que se han visto en los párrafos anteriores: cuando la cesión está autorizada en una ley; cuando se trate de datos recogidos de fuentes accesibles al público, cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique, cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.

Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas; cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos o cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Es muy importante destacar que aquel a quien se comunica los datos personales se obliga, por el sólo hecho de la comunicación a la observancia de las disposiciones existentes sobre Protección de Datos.

CALIDAD DE LOS DATOS

La Ley Orgánica 15/1999 contiene entre sus principios generales, el principio de calidad de los datos, que, ligado al principio de proporcionalidad de los datos, exige que los mismos sean adecuados a la finalidad que motiva su recogida.

La recogida y tratamiento de datos de carácter personal debe efectuarse desde su subordinación a los principios de calidad de los datos y de proporcionalidad que establece la Ley.

No puede obviarse que estamos tratando de un auténtico derecho fundamental, cuyo contenido el Tribunal Constitucional ha terminado de perfilar en las Sentencias 290/2000 y 292/2000, de 30 de noviembre, denominándolo derecho de autodeterminación informativa o de libre disponibilidad de los datos de carácter personal. Así, en dicha sentencia se indica que este derecho fundamental «persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado», estableciendo, en cuanto a su ámbito, que «el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto

no es sólo la intimidad individual, que para ello esta la protección que el artículo 18. 1 CE otorga, sino los datos de carácter personal».

De acuerdo con la consolida doctrina del Tribunal Constitucional[64], a la hora de limitar un derecho fundamental, hay que realizar un triple juicio a la hora de realizar la oportuna ponderación entre derechos, a saber:

— Juicio de idoneidad: la medida debe ser capaz de conseguir el fin pretendido.

— Juicio de necesidad: no debe existir otro medio o medida menos invasiva para alcanzar el fin pretendido.

— Juicio de proporcionalidad: tiene que provocar más beneficios que los perjuicios causados.

Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido[65]. Igualmente no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

La Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 9 de marzo de 2001, nos recuerda este principio: «Uno de los principios que inspira la legislación sobre tratamiento automatizado de datos de carácter personal es el de calidad de datos. Este principio implica, entre otras cosas, que los datos sean necesarios y pertinentes para la finalidad para la cal hubieran sido recabados o registrados (art. 4.5 de la LO 5/1992) y que sean exactos y completos art. 4.4 de la LO 5/1992. Por lo tanto, si los datos han dejado de ser necesarios para los fines para los cuales fueron recabados o registrados o resultan inexactos, se debe proceder (..) a su cancelación, sin necesidad de solicitud del afectado. Y así se infiere del propio tenor literal de los artículos 4.4 y 4.5 de la LO 5/1992, que utiliza la expresión imperativa "serán cancelados" y sin condicionarla a la existencia de una previa solicitud del afectado. En suma, la norma establece la obligación del responsable del fichero de proceder de oficio y con la debida diligencia a cancelar los datos inexactos o que han dejado de ser necesarios para la finalidad del fichero y sin necesidad de solicitud previa del afectado».

---

64 Véanse entre otras, STC 57/1999, STC143/1994 o 37/1998.

65 Téngase en cuenta el Dictamen 3/2013 del Grupo de Trabajo del Artículo 29 sobre limitación a la finalidad. De acuerdo al mismo los datos de carácter personal deberán ser recogidos para 'determinados, explícitos y legítimos' fines y no ser 'tratados posteriormente de manera incompatible con dichos fines (uso compatible).

En una sentencia posterior de 21 de enero de 2004 (recurso 1939/2001), la Audiencia Nacional indica que: «El principio de calidad del dato comienza a infringirse en el momento en que se facilitan datos erróneos a un fichero que presta información a terceros sobre el incumplimiento de obligaciones dinerarias. Así, como sostiene la sentencia del Tribunal Constitucional 254/1993, el Art. 18.4 de la CE, del que son desarrollo las Leyes Orgánicas 5/1992 y 1 5/1999, incorpora un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática».

También queremos destacar la Sentencia de la Audiencia Nacional de 3 de marzo de 2004 en la que manifiesta que: «como el previsto en el artículo 4.3 de la citada Ley que impone la veracidad y exactitud de los datos de carácter personal. Acorde con este principio se establecen una serie de obligaciones, tendentes a alcanzar esa veracidad y exactitud de los datos de carácter personal que se encuentran en el fichero, y cuyo incumplimiento es digno de reproche y con figura una infracción administrativa por la que se impone la sanción que se recurre».

MEDIDAS DE SEGURIDAD

El Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, establece las medidas de seguridad en el tratamiento de datos de carácter personal.

Debe tenerse en cuenta que esta obligación trae causa del deber de secreto regulado en el artículo 10 de la LOPD y que como reza la Audiencia Nacional, en sentencias, entre otras, de fechas 14 de septiembre de 2001 y 29 de septiembre de 2004 lo siguiente: «este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE.

Las medidas de seguridad se clasifican en tres niveles: básico, medio y alto, en función del nivel de seguridad de los datos objeto de tratamiento, siendo estas medidas acumulativas. Así lo establece el artículo 81 del citado Real Decreto, que señala que todos los ficheros de datos personales deberán ser objeto de medidas de seguridad básicas, debiendo aplicar éstas y las de nivel medio en los ficheros o tratamientos siguientes:

Los «relativos a la comisión de infracciones administrativas o penales» y «prestación de servicios de información sobre solvencia patrimonial y crédito».

Aquellos de los que sean responsables «Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias», «las entidades financieras para finalidades relacionadas con la prestación de servicios financieros», y «las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias», así como «aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social».

Por último, los ficheros «que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos».

Las medidas de nivel alto de seguridad, junto con las de nivel básico y medio, han de llevarse a cabo en los ficheros o tratamientos «que se refieran a datos de ideología, afiliación sindical,

religión, creencias, origen racial, salud o vida sexual», salvo cuando los datos «se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros», o «se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad», en cuyo caso se aplicarán las medidas de seguridad básicas. Éstas serán aplicables también en los datos de salud que hagan referencia «exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado».

También serán objeto de medidas de seguridad de nivel alto los ficheros «que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas», «aquéllos que contengan datos derivados de actos de violencia de género», y «de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas (…) respecto a los datos de tráfico y a los datos de localización».

Los Capítulos III y IV del Reglamento detallan de forma concisa las medidas de seguridad correspondientes a cada nivel, y dividiéndolas entre ficheros automatizados y no automatizados. Dependiendo del nivel de seguridad se deben implementar las siguientes medidas[66]:

Automatizados

— Nivel Básico: Funciones y obligaciones del personal, registro de incidencias, control de acceso, gestión de soportes y documentos, identificación y autenticación, copias de respaldo y recuperación.

— Nivel Medio: responsable de seguridad, auditoría bienal, gestión de soportes y documentos, identificación y autenticación, control de acceso físico, registro de incidencias.

— Nivel Alto: gestión y distribución de soportes, copias de respaldo y recuperación, registro de accesos, telecomunicaciones.

No automatizados

— Nivel Básico: obligaciones comunes, criterios de archivo, dispositivos de almacenamiento, custodia de los soportes.

— Nivel Medio: responsable de seguridad, auditoría.

— Nivel Alto: almacenamiento de la información, copia o reproducción, acceso a la documentación, traslado de documentación.

Como novedad en este apartado, queremos reseñar que estamos a la espera de la versión definitiva de la Guía para la Evaluación de Impacto en Datos Personales (EIPD), cuyo borrador[67] fue presentada en la 6.ª Sesión Anual Abierta de la AEPD, y que posteriormente ha sido sometida a un proceso de consulta pública. Aún no siendo obligatoria esta figura en la normativa española, en palabras del Director de la AEPD durante la presentación de la misma, su adopción será valorada positivamente por la AEPD a la hora de valorar el grado de cumplimiento de la LOPD por parte de la entidad o administración pública que la pone en marcha.

HABEAS DATA Y DERECHOS ARCO

El *habeas data* es una acción constitucional que puede ejercer cualquier persona que estuviera incluida en un registro o banco de datos, para acceder a tal registro y que le sea

---

66 Para más información, véase la «Guía de Seguridad de Datos–2010». http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf.

67 http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GuiaEIPDPBorrador.pdf.

suministrada la información existente sobre su persona, y de solicitar la eliminación o corrección si fuera falsa o estuviera desactualizada.

La Acción del *habeas data* nace como instrumento para salvaguardar el derecho a su honor e intimidad, dando a las personas la posibilidad de conocer la información que existe sobre sí mismas en los registros de datos, así como a eliminarla, modificarla o limitar su uso.

Es la esfera más íntima de la persona, la que las diferentes Constituciones de los Estados pretenden proteger, dotando a las personas de instrumentos jurídicos y acciones que les permitan proteger sus derechos.

La Constitución Española de 1978, en su artículo 18, así lo reconoce:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Como ya ha sido comentado, el texto constitucional se desarrolla por la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal, y en sus artículos 15 y 16 reconoce los derechos de acceso, cancelación y rectificación, estableciendo sobre el derecho de acceso, que el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. Así mismo se tratan los derecho de rectificación y cancelación: «serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos».

Pasamos a resumir de forma esquemática a continuación cada uno de los derechos que configuran el *Habeas Data* en España:

Derecho de Acceso

El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

— Justificación: no es necesaria, salvo si se ha ejercitado el derecho en los últimos doce meses.

— Plazos: El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. El acceso podrá hacerse efectivo durante 10 días hábiles tras la comunicación de la resolución.

— Denegación: debe motivarse e indicar que cabe invocar la tutela de la AEPD. Son motivos de denegación que el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud (salvo que se acredite un interés legítimo al efecto) y que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de sus datos.

Derecho de Rectificación

Derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

— Justificación: debe indicarse a qué datos se refiere y la corrección que haya de realizarse aportando documentación.

— Plazo: 10 días hábiles.

— Denegación: debe motivarse y procede indicar que cabe invocar la tutela de la AEPD.

Derecho de Cancelación

Derecho del afectado a que se supriman los datos que resulten ser inadecuados o excesivos.

— Justificación: debe indicarse el dato a cancelar y la causa que lo justifica, aportando documentación.

— Plazo: 10 días hábiles.

— Denegación: debe motivarse y procede indicar que cabe invocar la tutela de la AEPD. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos, manteniéndose en esos casos debidamente bloqueados hasta la finalización de esos plazos.

Derecho de Oposición

Derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los supuestos en que no sea necesario su consentimiento para el tratamiento, que se trate de ficheros de prospección comerciales o que tengan la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en le tratamiento automatizado de sus datos.

— Justificación: concurrencia de motivos fundados y legítimos relativos a su concreta situación personal.

— Plazo: 10 días hábiles.

— Denegación: debe motivarse e indicar que cabe invocar la tutela de la AEPD.

Derecho al olvido

Sobre la base del derecho de oposición, la Agencia Española de Protección de Datos ha venido entendiendo sobre todo en actos de inserción obligatoria en Diarios Oficiales que la persona afectada tiene reconocido el derecho de oposición al tratamiento de sus datos de carácter personal bajo determinados requisitos y que el Diario o Boletín Oficial deben implantar tras el ejercicio de este derecho, mecanismos que impidan la futura indexación de los datos por buscadores, pero ante las reclamaciones dirigidas a los buscadores, y ante la negativa sistemática por parte de Google de retirar del Índice determinados resultados de búsqueda basados en el nombre y apellidos de un supuesto afectado, la AEPD ha resuelto multitud de procedimientos de tutela de derechos, como el Procedimiento n.º: TD/01768/2011, recurridos ante la jurisdicción contencioso-administrativo que acaban con la cuestión prejudicial planteada desde el Tribunal Supremo ante el TJUE que estima y respalda los argumentos de la AEPD y el español Mario Costeja González en la ya conocida y citada en esta obra STJUE C-131/2012 y que en su aplicación está empezando a producir fallos como la reciente sentencia de la AP de Barcelona 364/2014 que condena a Google a pagar una indemnización de 8.000€ por indexar la publicación de un indulto en el BOE.

Derecho de exclusión

Para finalizar este epígrafe, señalaremos brevemente con el fin de conciliar el derecho a la protección de datos de carácter personal con lo dispuesto para la posibilidad de realizar tratamientos de datos obtenidos de fuentes accesibles al público[68], el Real Decreto 1720/2007 regula en sus artículos 45 a 51 el denominado «derecho de exclusión», lo que ha llevado a la creación de las denominadas listas Robinson[69], donde los particulares pueden indicar su deseo de no recibir publicidad y por qué canal no desean recibirla, debiendo las empresas de publicidad consultarlas antes de realizar labores de publicidad.

ENCARGADOS DE TRATAMIENTO Y *CLOUD COMPUTING*

La figura del Encargado de Tratamiento viene definida en el art. 3 de la LOPD como: «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento». En nuestra opinión, resulta mucho más definitorio el nombre otorgado a Responsables y Encargados de Tratamiento en la versión en ingles de la Directiva 95/46/CE, que los denomina *Data Controllers* y *Data Processors* respectivamente.

Por tanto, se trata de un tercero distinto al Responsable del Fichero que tiene acceso a datos personales del mismo necesarios para la prestación de un servicio, sin ser un cesionario según la definición legal del término.

Según el art. 12 de la LOPD, este tratamiento de datos «deberá estar regulada en un contrato (…) estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas», debiendo destruir o devolver al Responsable los datos objetos de tratamiento.

Asimismo, el Encargado deberá implementar las medidas de seguridad correspondientes al Responsable del Fichero.

Por ultimo, añade el art. 12 que será considerado Responsable del tratamiento y por tanto de las infracciones cometidas en caso de que «destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato».

Por su parte, el Capítulo III del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, regula la subcontratación de servicios por parte del Encargado de Tratamiento, señalando que requerirá la autorización del Responsable, y «la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento», salvo que «se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar». Si no se identifica la

---

68 Definidos en el artículo 3 j) de la LOPD como: «aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación».

69 www.listarobinson.es.

empresa, se requerirá que «comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación».

También se acepta la autorización previa por parte del Responsable cuando el tratamiento por parte del subcontratista «se ajuste a las instrucciones del responsable del fichero», y cuando «el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior». En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

En última instancia el art. 21.3 señala que «si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior».

Un ejemplo claro y actual de la figura del Encargado de Tratamiento es la de los prestadores de servicios de «*Cloud Computing*» o computación en la nube.

La computación en la nube son un conjunto de tecnologías que permiten una serie de servicios computacionales a través de Internet (la «nube»). En un entorno de *cloud computing* la gestión de la información está de forma virtual en manos del cliente que contrata los servicios de la nube a una empresa de «cloud», que la trata a través de Internet accediendo a soluciones de bases de datos, correo electrónico, nóminas o gestión de recursos humanos de acuerdo a sus necesidades. Como consecuencia de lo anterior, el mismo contratista puede desconocer la localización precisa de sus datos y no disponer del control directo de acceso a los mismos, de su borrado y de su portabilidad, ya que la información no está físicamente en su poder aunque, si esa información contiene datos de carácter personal, sí está bajo su responsabilidad desde el punto de vista de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD). Téngase en cuenta que en la contratación de estos servicios existe una obligación «in vigilando» que puede llevar intrínseca la obligación de no contratar con un proveedor de servicios que no ofrezca estas garantías[70]».

El prestador de servicios de *cloud computing*, en su calidad de prestador de servicios con acceso a datos personales, es un Encargado de Tratamiento, y por tanto, está sujeto a las obligaciones ya desglosadas en el apartado correspondiente. En particular, adquieren aquí especial relevancia las obligaciones relativas a la subcontratación, ya que como hemos visto en la mayoría de los casos el prestador de servicios de «cloud» trata o almacena los datos a través de medios o infraestructuras de terceros.

AUTORIDADES DE CONTROL. INSCRIPCIÓN O REGISTRO DE TRATAMIENTO

La Directiva 95/46/CE establece que en todos los Estados miembros exista, al menos, una autoridad independiente que controle y garantice el Derecho Fundamental a la protección de datos.

En España la Agencia Española de Protección de Datos es el ente de derecho público que vela por el cumplimiento de la normativa sobre protección de datos personales. Según el mandato europeo, informa sobre el contenido, los principios y las garantías del derecho

---

[70] Deben tomarse en cuenta en este sentido las Guías de la AEPD: Guía para clientes que contraten servicios de *Cloud Computing* y Orientaciones para prestadores de servicios de *Cloud Computing* disponibles en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php.

fundamental a la protección de datos, tutelando al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos por los responsables de los ficheros, y ejerciendo la potestad sancionadora ante las actuaciones de los responsables o encargados de ficheros que puedan ser contrarias a los principios y garantías contenidos en la LOPD.

Entre sus funciones, reguladas en el artículo 37 de la LOPD podemos destacar: velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos, emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias, atender las peticiones y reclamaciones formuladas por las personas afectadas, proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal o ejercer la potestad sancionadora derivada de las actuaciones de inspección llevadas a cabo con anterioridad.

El Registro General de Protección de Datos es el órgano al que corresponde velar por la publicidad de la existencia de los ficheros que contengan datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, regulados en los artículos 14 a 16 de la LOPD.

De acuerdo con el artículo 26 de la LOPD, «Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos».

Además, de conformidad con el artículo 39 de la citada Ley, serán también objeto de inscripción en el Registro las autorizaciones de transferencias internacionales, los códigos tipo, los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Téngase en cuenta que el acceso a la información contenida en este Registro será pública y gratuita para cualquier persona que podrá conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

Actualmente contamos además con una figura que no ha sido muy utilizada pero que es un buen punto de partida para el futuro Sello Europeo de Protección de Datos, recogido en la Propuesta de Reglamento General de Protección de Datos, tal y como se verá en el Capítulo correspondiente, siendo los denominados Códigos Tipo. Regulados en el artículo 32 de la LOPD, tendrán el carácter de códigos deontológicos o de buena práctica profesional, pudiendo contener el «régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo». Los mismos deberán ser inscritos en el Registro General de Protección de Datos de la AEPD u organismo autonómico equivalente, en su caso. Podrán crearlos tanto responsables de titularidad pública como privada, mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa.

Para finalizar indicaremos que el artículo 41 de la LOPD permite la creación de autoridades de control por parte de las Comunidades Autónomas que ejercerán ciertas competencias atribuidas a la AEPD en su territorio, eso sí únicamente sobre los ficheros de Titularidad Pública, pudiendo crear su propio Registro de Ficheros de Protección de Datos. En la actualidad

Cataluña[71] y País Vasco[72] cuentan con Agencia Autonómica, Madrid[73] la tuvo y Andalucía acaba de crear el Consejo de Transparencia y Protección de Datos de Andalucía[74], aunque aún no se ha puesto en funcionamiento.

TIPOS DE PROCEDIMIENTOS

El Reglamento de Protección de Datos (RD 1720/2007) contempla los siguientes procedimientos que son objeto de tramitación ante la Agencia Española de Protección de Datos:

— Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición.

— Procedimientos relacionados con la inscripción o cancelación de ficheros.

— Procedimientos relacionados con las transferencias internacionales de datos.

— Procedimiento de inscripción de códigos tipo.

— Procedimiento de exención del deber de información al interesado.

— Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos.

PROCEDIMIENTO SANCIONADOR

Los arts. 43 a 49 de la LOPD regulan el procedimiento sancionador, que se inicia contra los responsables de ficheros cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD.

Este procedimiento arranca de oficio mediante acuerdo del Director de la Agencia cuando existan pruebas razonables de que se ha producido alguna infracción de los principios y garantías contenidos en la LOPD.

Normalmente el acuerdo de iniciación se origina como consecuencia de una denuncia realizada por un ciudadano o de un tercero.

---

71 Creada por la Ley 5/2002, en la actualidad su marco jurídico, competencias y funciones se encuentran reguladas en el Decreto 48/2003, de 20 de febrero, por el cual se aprueba el Estatuto de la Agencia Catalana de Protección de Datos y la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos que deroga la Ley 5/2002.

72 Creada por la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos. También la regulan el Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, el Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos y la Resolución de 21 de julio de 2005, del Director de la Agencia Vasca de Protección de Datos, por la que se establecen los modelos normalizados y los medios por los que debe procederse a la solicitud de las inscripciones de creación, modificación o supresión de ficheros en el Registro de Protección de Datos de la Agencia Vasca de Protección de Datos.

73 Creada por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, se encuentra derogada por la Disposición Derogatoria Única de la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas de la Comunidad Autónoma de Madrid.

74 Mediante la Ley 1/2014 de 24 de junio, de Transparencia Pública de Andalucía se crea este órgano siendo una se sus funciones, de acuerdo con el artículo 45, el control en materia de protección de datos en los términos previstos en el artículo 41 de la Ley Orgánica 15/1999, de 13 de diciembre.

En otras ocasiones se debe al conocimiento por parte de la AEPD de un hecho presuntamente ilícito, por ejemplo, a través de alguna noticia aparecida en los medios de comunicación social.

La AEPD investiga la denuncia y puede suspender temporalmente el tratamiento. En caso de concluir que se ha violado la LOPD la Agencia puede ordenar la supresión o destrucción de los datos o prohibir el tratamiento.

INFRACCIONES Y RÉGIMEN DE SANCIONES

En la legislación española, las sanciones oscilan entre 900 a 40.000 euros para infracciones leves, 40.001 a 300.000 euros para las graves, y 300.001 a 600.000 euros las muy graves. Estas sanciones son únicamente impuestas a los tratamientos de titularidad privada (empresas, empresarios individuales, otras entidades con personalidad jurídica…), puesto que para los tratamientos de titularidad pública (aquellos gestionados por administraciones e instituciones públicas), conforme a lo dispuesto en el artículo 46 de la LO 15/1999, el órgano sancionador dictará una resolución que recoja las medidas a adoptar para que se corrijan o cesen los efectos de la infracción y, en su caso, podrá iniciar actuaciones disciplinarias.

El art. 44 de la LOPD clasifica las infracciones en:

Leves

— No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo.

— No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

— El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.

— La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.

Graves

— Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o diario oficial correspondiente.

— Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo.

— Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.

— La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.

— El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

— El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.

— El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo.

— Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

— No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.

— La obstrucción al ejercicio de la función inspectora.

— La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

Muy graves

— La recogida de datos en forma engañosa o fraudulenta.

— Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.

— No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.

— La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria.

Si la infracción se tipifica como leve o grave, y el infractor no hubiera sido sancionado o apercibido con anterioridad, con carácter excepcional, atendiendo a las circunstancias del hecho y previa audiencia de las partes, puede no iniciar el procedimiento sancionador sustituyéndolo por un apercibimiento al infractor en el que se le obligue a acreditar en un plazo determinado, la implantación de medidas correctoras. Si transcurrido el citado plazo no se hubiera atendido el apercibimiento, el órgano sancionador puede iniciar procedimiento por incumplimiento.

En lo que respecta a la graduación de la cuantía de las sanciones, el artículo 45.4 de la Ley Orgánica 15/1999 establece una serie de criterios para su baremo, como son, el carácter continuado, el volumen de los datos afectados o el beneficio obtenido. También se puede imponer la sanción en la escala precedente en gravedad, si concurre alguno de los supuestos reflejados en el artículo 45.5.

Para finalizar comentaremos que los plazos de prescripción tanto de las infracciones, como de las sanciones son de tres años para las muy graves, dos años para las graves y un año para las leves, computándose los plazos desde el día en que la infracción se ha cometido o la sanción adquiere firmeza.

OTRA LEGISLACIÓN APLICABLE

No resulta tarea sencilla tratar de sintetizar en un apartado otras normas que regulan aspectos relacionados con la protección de datos de carácter personal debido a que es raro encontrar a un sector que no tenga incidencia en este derecho fundamental. Es por ello que destacaremos los que se consideran más relevantes, de acuerdo con el contenido, estructura y fines de este Estudio, no siendo tampoco exhaustivos en la enumeración de todas y cada una de

las normas que inciden en ese sector, sino que destacaremos aquellas que consideremos más relevantes.

En materia de telecomunicaciones y comunicaciones electrónicas y servicios de la sociedad de la información, contamos con la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones[75] con disposiciones especiales en materia de protección de datos, obligación de notificación de quiebras de seguridad, derecho de exclusión de la Guía de abonados o retención de datos, entre otros, motivados por la especial regulación que hay en esta materia desde la entrada en vigor de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). En esta misma línea la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[76] que obliga a mantener cierta información de tráfico de datos durante un periodo de 12 meses. No podríamos finalizar este apartado sin una somera referencia a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico[77], fijando reglas sobre consentimiento y validez de comunicaciones promocionales por vía electrónica y regulando la manera en la que se debe facilitar información y obtener el consentimiento al instalar dispositivos de almacenamiento y recuperación de datos, entre los que se encuentran las famosas «cookies».

Desde el punto de vista de la Administración Pública, del acceso a información y documentación pública y transparencia, tenemos la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[78] que habilita una serie de cesiones de datos al obligar a su publicación y regula el derecho de acceso a documentación pública por parte de los ciudadanos, fijando su alcance, límites, contenido y procedimiento. Por su parte el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español[79] regula los plazos para el acceso a documentos que puedan atentar contra la intimidad de los ciudadanos.

En otro orden de cosas, el artículo 61 de la Ley 30/1992, de 26 de noviembre, Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común[80] permite al órgano competente si aprecia que la notificación por anuncio o publicación en Diario Oficial lesiona derechos e intereses legítimos a que pueda publicar una somera indicación del contenido junto con el lugar y plazo donde pueden conocer el contenido íntegro del mismo.

Por su parte el artículo 70 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local[81] declara secretas las sesiones de la Junta de Gobierno en contraposición a las sesiones del Pleno que son públicas, aunque podrán ser secretos aquellos puntos que puedan atentar contra el derecho a la intimidad del artículo 18.1 de la Constitución Española. De igual forma los ciudadanos tienen derecho a obtener copias y certificaciones de los acuerdos de las corporaciones, pudiéndose denegar mediante resolución motivada si afectara, entre otros supuestos, a la intimidad de las personas.

---

75 BOE núm. 114 de 10 de mayo de 2014.
76 BOE núm. 251 de 19 de octubre de 2007.
77 BOE núm. 166 de 12 de julio de 2002.
78 BOE núm. 295 de 10 de diciembre de 2013.
79 BOE de 29 de junio de 1985.
80 BOE n.º 285, 27-nov-1992.
81 BOE de 03 de julio de 1985.

En lo que respecta al tratamiento de datos de salud, no se puede obviar la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica[82], al regular el contenido de la historia clínica y permitir el acceso a la misma por parte de su titular. También regula su modo de conservación y plazos y quienes están habilitados a acceder a la misma.

Tratándose de videovigilancia tenemos por un lado la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras[83] de la que cabe destacar el modo de cumplir con el deber de información a través de un logotipo diseñado para tal efecto con su correspondiente texto legal, y el plazo máximo de un mes de conservación de imágenes.

En el supuesto que el sistema de videovigilancia se utilice con fines de seguridad privada, se estará a lo dispuesto en el artículo 42 de la Ley 5/2014, de 4 de abril, de seguridad privada[84], pudiendo acceder a esos sistemas únicamente vigilantes de seguridad o guardias rurales en su caso, salvo que se trate de un sistema de autoprotección personal, de acuerdo con la excepción prevista en el artículo 7 de citada ley. De estar situadas las cámaras en zonas exteriores se estará a lo dispuesto en la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos[85] que obliga a solicitar autorización previa a la Comisión de Garantías de Videovigilancia constituida en el seno de la Delegación del Gobierno en cada Comunidad Autónoma. Además de la habilitación legal a Fuerzas y Cuerpos de Seguridad del Estado, tras la entrada en vigor de la Ley 5/2014 de seguridad privada, estas empresas pueden solicitar la autorización, y una vez obtenida instalar y manejar estos sistemas con cámaras exteriores.

También es digno de mención en este apartado reseñar la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo[86] y su desarrollo reglamentario mediante el Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo[87]. Cabe destacar que esta normativa obliga a realizar bajo el paraguas de la «diligencia debida» determinados tratamientos de datos personales, así como labores de identificación y documentación. Es igualmente destacable que quiebra el principio de deber de información y obtención del consentimiento de los artículos 5 y 6 de la Ley Orgánica 15/1999, no siendo aplicables a estos supuestos.

También regula las cesiones de datos a través de la figura de la comunicación por indicio al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, por lo que no se requerirá el consentimiento expreso del afectado conforme al artículo 11 de la Ley Orgánica 15/1999.

Sin existir legislación sectorial al efecto[88], pero entendiendo que el tema es digno de mención por la relevancia de la jurisprudencia en la materia, creemos que este Estudio quedaría incompleto sin unas notas a la disyuntiva entre privacidad o uso de mecanismos de control empresarial. Téngase en cuenta, independientemente de si se trata de monitorización de equipos, acceso al correo electrónico, instalación de sistemas de geolocalización en vehículos o uso de

---

82 BOE n.º 274, 15-nov-2002.
83 BOE núm. 296 de 12 de diciembre de 2006.
84 BOE núm. 83 de 05 de abril de 2014.
85 BOE de 05 de agosto de 1997.
86 BOE núm. 103 de 29 de abril de 2010.
87 BOE núm. 110 de 06 de mayo de 2014.
88 En materia de relaciones laborales y para otros aspectos que no destacamos en este apartado contamos con la «Guía "La protección de datos en las relaciones laborales" – 2009». http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php.

imágenes para otras finalidades, de la obligación de ser transparentes en la información que se facilita con carácter previo a los trabajadores y a sus representantes. En este sentido la Sentencia 29/2013 del Tribunal Constitucional declara nulo el despido de un trabajador al usar como prueba las grabaciones de un sistema de videovigilancia sin haber informado antes a los trabajadores y sus representantes de este uso de las imágenes adicional al principal (seguridad). O en lo relativo al acceso al correo electrónico profesional, equipos informáticos o programas de monitorización, las Sentencias del Tribunal Supremo de 26 de septiembre de 2007[89] y 6 de octubre de 2011[90] o las Sentencias del Tribunal Constitucional STC 241/2012[91] y 170/2013[92].

Más recientemente en la jurisdicción penal la Sentencia 2844/2014, de 16 de junio, que a través de un Obiter Dicta, establece su doctrina sobre el acceso al correo electrónico profesional y su validez como prueba en un proceso penal. Diferencia dos supuestos, que el correo electrónico ya esté abierto por lo que entra en juego el 18.1 de la CE y lo establecido para estos supuestos por la jurisprudencia estudiada anteriormente, y lo que supone una gran novedad, lo previsto para los correos electrónico aún sin abrir por el destinatario. En estos últimos entiende el TS que lo que está en juego es el secreto de las comunicaciones regulado en el artículo 18.3 de la CE, por lo que únicamente se podrá acceder a estos correos mediante «intervención judicial».

Para finalizar indicaremos que determinados actos o conductas que puedan atentar contra la seguridad de los datos o la integridad de los mismos, pueden ser considerados delitos, de acuerdo con la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal[93], al regular el delito de descubrimiento y revelación de secretos en los artículos 197 a 201 y el delito de daños informáticos en el artículo 264.

2.7 MÉXICO

Constitución Política

Artículo 6: La información sobre la vida privada y los datos personales en los archivos gubernamentales serán protegidos conforme a las leyes secundarias.

BIEN JURÍDICO PROTEGIDO: DEFINICIÓN DE DATO DE CARÁCTER PERSONAL

En la Ley Federal de Protección de Datos Personales en posesión de los Particulares (LFPDPPP) se establece que el objeto de la dicha Ley es la protección de los datos personales en

---

89 El Tribunal dispone que «en síntesis prevé la posibilidad de que el empresario pueda acceder al control del ordenador, del correo electrónico y los accesos a Internet de los trabajadores, siempre que la empresa de buena fe haya establecido previamente las reglas de uso de esos medios con aplicación de prohibiciones absolutas o parciales e informado de que va existir un control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos».

90 Da un paso más al establecer que «si la empresa prohíbe totalmente el uso de estas tecnologías con fines particulares, ya sea dentro o fuera del horario laboral, no se puede entender que el Derecho Fundamental a la Intimidad o al Secreto de las comunicaciones opera en el uso de estos equipos».

91 Disponiendo que ante el acceso a un programa de chat instalado por las propias trabajadoras en un equipo multiusuario no cabe alegar expectativa en privacidad.

92 El TC ratifica el despido disciplinario de un trabajador de una empresa del sector químico que estaba pasando información a la competencia mediante el correo electrónico profesional. La empresa accedió al correo electrónico del trabajador y en base a ello lo despidió disciplinariamente. El TC entiende que como el Convenio Colectivo de las empresas del sector químico establece que los medios informáticos son medios profesionales, debe entenderse prohibido el uso personal de los mismos.

93 BOE núm. 281 de 24 de noviembre de 1995.

posesión de los particulares, siendo estos definidos como: «Cualquier información concerniente a una persona física identificada o identificable»[94].

Cabe hacer mención que aunque la definición anterior nos hace referencia a que los datos personales son los correspondientes a una persona física, existe una tesis aislada que tales datos personales a las personas jurídicas o morales, ya que la misma establece: «personas morales. tienen derecho a la protección de los datos que puedan equipararse a los personales, aun cuando dicha información haya sido entregada a una Autoridad»[95].

Esta tesis establece la posibilidad de que los derechos de protección de los datos personales, tales como el control de los individuos sobre el acceso y uso de sus datos personales también puede extenderse a cierta información de las personas morales.

Es entonces cuando se habla de la protección de información y documentos inherentes a las personas morales, tales como información comercial, económica o relacionada con la identidad de las personas morales. Pero la duda es porque se habla de que la protección de esta información es una extensión del derecho a la protección de los datos personales de las personas físicas, cuando este derecho ya se encontraba protegido por los derechos de privacidad, confidencialidad y sobre todo, de protección del secreto industrial.

INFORMACIÓN Y CONSENTIMIENTO. OBLIGACIÓN DE TRANSPARENCIA

Principio de información[96]

Conforme a la legislación mexicana se establece la obligación para el responsable del tratamiento de los datos personales (el responsable) el que dé a conocer al titular de los datos la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales, ello a través del aviso de privacidad.

Ahora bien, para que dicho aviso de privacidad sea adecuado conforme a la LFPDPPP y a su correspondiente reglamento (RLFPDPPP), el mismo deberá ser sencillo, con la información necesaria, expresado en lenguaje claro y comprensible, con una estructura y diseño que facilite su entendimiento, y contendrá al menos lo siguiente:

— Identidad y domicilio del responsable que los recaba.

— Las finalidades del tratamiento de datos.

— Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos.

— Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición (ARCO).

— Las transferencias de datos que en su caso se efectúen.

---

94 Artículo 3, fracción V de la LFPDPPP.

95 Tesis P. II/2014 (10a.), Pleno, publicada en la Gaceta del Semanario Judicial de la Federación en junio del 2014, Libro 3, Décima Época, p.p. 274, tesis aislada (constitucional), consultada el 05 de julio del 2014 de: http://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=protecci%25c3%25b3n%2520de%2520datos%2520personales&Dominio=Rubro&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=5&Epp=20&Desde=-100&Hasta=-100&Index=0&ID=2005522&Hit=2&IDs=2006753,2005522,2004341,2000238,169167&tipoTesis=&Semanario=0&tabla=.

96 Artículos 15 al 18 de la LFPDPPP y 23 al 31 del RLFPDPPP.

— El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad.

— En el caso de datos personales sensibles, señalará expresamente que se trata de este tipo de datos.

La puesta a disposición del aviso de privacidad por parte del responsable y para titulares, debe realizarse a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

— Cuando los datos sean obtenidos personalmente del titular, el aviso será facilitado en el momento en que se recaba el dato.

— Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable proporcionará al titular de manera inmediata, al menos (a) la identidad y domicilio del responsable, (b) las finalidades del tratamiento y (c) los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

— Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad. Excepto cuando el tratamiento sea con fines históricos, estadísticos o científicos.

— Cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, previa autorización del Instituto Federal de Acceso a la Información y Protección de Datos Personales (Instituto), el responsable podrá instrumentar medidas compensatorias.

Principio de consentimiento[97]

Para poder realizar el tratamiento de los datos personales, siempre se requerirá el consentimiento de su titular, excepto en los siguientes casos:

— Esté previsto en una Ley.

— Los datos figuren en fuentes de acceso público.

— Los datos se sometan a un procedimiento previo de disociación.

— Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.

— Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.

— Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la legislación en materia de salud y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente.

— Se dicte resolución de autoridad competente.

Ahora bien, conforme a la legislación mexicana el consentimiento puede ser de dos formas:

Expreso: se da cuando la voluntad del titular se manifiesta verbal, por escrito —firma autógrafa, huella dactilar, firma electrónica o cualquier mecanismo o procedimiento que

---

97 Artículos 8 al 10 de la LFPDPPP y 11 al 21 del RLFPDPPP.

permita identificar al titular y recabar su consentimiento—, por medios electrónicos, ópticos, por otra tecnología, o por signos inequívocos.

Así mismo, el responsable deberá obtener el consentimiento expreso por parte del titular, tratándose de:

— Datos financieros o patrimoniales, salvo las excepciones marcadas por la ley.

— Datos personales sensibles, en donde además de obtener el consentimiento expreso, se establece que el mismo se debe obtener por escrito, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

— Cuando lo exija la legislación.

— Lo solicite el responsable para acreditar dicho consentimiento.

— Lo acuerden entre el titular y el responsable.

Tácito: se lleva a cabo cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición. Esta forma de consentimiento será aplicado como regla general, salvo los casos en los que la legislación exija el consentimiento expreso.

Para que el consentimiento tácito tenga validez, se deberá de cumplir con lo siguiente:

— Cuando los datos personales se recaben de forma directa o personalmente de su titular, se pondrá previamente a disposición el aviso de privacidad. Este Aviso contendrá el mecanismo para que el titular pueda manifestar su negativa al tratamiento de sus datos para las finalidades que sean distintas a aquellas que son necesarias y den origen a la relación jurídica entre el responsable y el titular.

— Cuando los datos personales se obtengan de manera indirecta del titular y cambien las finalidades del tratamiento, el responsable pondrá a disposición del titular el aviso de privacidad previo al aprovechamiento de los datos personales.

— Cuando el aviso de privacidad no se haga del conocimiento del titular de manera directa o personal, el titular tendrá un plazo de 5 días para que manifieste su negativa para el tratamiento de sus datos para las finalidades que sean distintas a las que son necesarias y den origen a la relación jurídica entre el responsable y el titular.

— Si el titular no manifiesta su negativa para el tratamiento de sus datos, se entenderá que ha otorgado su consentimiento para el tratamiento de los mismos, salvo prueba en contrario.

Sea que el consentimiento se obtenga de manera expresa o tácita, el mismo deberá cumplir con las siguientes características:

— Libre: es decir, que su obtención debe ser sin que medie error, mala fe, violencia o dolo.

— Específica: debe ser referida a una o varias finalidades determinadas que justifiquen el tratamiento.

— Informada: el titular deberá tener conocimiento del aviso de privacidad previo al tratamiento de sus datos personales, así como de las consecuencias de otorgar su consentimiento.

— Inequívoco: en el caso del consentimiento expreso, este deberá a su vez ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento.

Respecto al momento en el que se tiene que llevar a cabo la obtención del consentimiento, en los casos en los que los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.

La revocación del consentimiento podrá llevarse a cabo en cualquier momento y sin que se le atribuyan efectos retroactivos. Para ello, el responsable deberá establecer en el aviso de

privacidad los mecanismos y procedimientos sencillos y gratuitos que permitan al titular revocar su consentimiento.

DATOS ESPECIALMENTE PROTEGIDOS Y OTROS TRATAMIENTOS INVASIVOS

Como fue referido en el apartado de Consentimiento, los datos especialmente protegidos y los cuales requieren consentimiento expreso para su tratamiento son:

— Los datos personales sensibles, los cuales son los que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual[98].

— Los datos financieros y patrimoniales.

Otra mención especial se establece con respecto a la obligación de que dentro de las finalidades del tratamiento se incluirán las relativas al tratamiento para fines mercadotécnicos, publicitarios o de prospección comercial.

CESIONES DE DATOS[99]

En la legislación mexicana en materia de protección de datos personales no existe como tal el concepto de cesión de datos. Sin embargo la figura que pueden equiparse a la cesión por el hecho de incluir toda revelación de datos personales realizada de manera distinta al titular de los datos personales es la transferencia.

Transferencia. La cual es toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento[100].

Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá cumplir con lo siguiente:

— Comunicar a tercero el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.

— El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad del responsable, mismo que contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos.

— El tercero receptor asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

El consentimiento para la transferencia de los datos personales, tendrá las siguientes excepciones, por lo que dicha transferencia podrá llevarse a cabo sin el consentimiento del titular cuando:

— Esté prevista en una Ley o Tratado internacional.

— Sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.

---

98 Artículo 3 fracción VI de la LFPDPPP.
99 Artículos 36 y 37 de la LFPDPPP y 67 al 76 del RLFPDPPP.
100 Artículo 3 fracción XIX de la LFPDPPP.

— Sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas.

— Sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.

— Sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia.

— Sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

— Sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

Una vez que el tercero recibe los datos personales, se convierte a su vez en responsable del tratamiento, por lo que deberá tratar los datos personales conforme a lo convenido en el aviso de privacidad que le comunique el responsable transferente.

CALIDAD DE LOS DATOS[101]

El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados para los fines para los cuales fueron recabados, para lo cual, el responsable adoptará los mecanismos necesarios para procurar que los datos personales permanezcan con tales características.

Existe una presunción de que se cumple con el principio de calidad cuando los datos personales son proporcionados directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga.

DERECHOS ARCO[102]

Los titulares de los datos personales o su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los mismos. Los cuales podrán ser ejercidos cuando:

— Acceso. Derecho de acceder a sus datos personales y a conocer el Aviso de Privacidad al que está sujeto el tratamiento.

— Rectificación. Se podrán rectificar los datos personales cuando sean inexactos o incompletos.

— Cancelación. Esta cancelación dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. Pudiendo conservarse solo para dar cumplimiento a las responsabilidades nacidas del tratamiento. Una vez cancelado el dato se dará aviso a su titular.

La cancelación de los datos personales no podrá ser llevada a cabo cuando los datos personales:

— Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento.

— Deban ser tratados por disposición legal.

---

101 Artículos 11 de la LFPDPPP y 36 del RLPDPPP.

102 Artículos 28 al 35 de la LFPDPPP y 101 al 111 del RLPDPPP.

— Obstaculicen actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.

— Sean necesarios para proteger los intereses jurídicamente tutelados del titular.

— Sean necesarios para realizar una acción en función del interés público.

— Sean necesarios para cumplir con una obligación legalmente adquirida por el titular.

— Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Oposición. El titular podrá en todo momento y por causa legítima a oponerse al tratamiento de sus datos.

MEDIDAS DE SEGURIDAD[103]

Los responsables deberán establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Estas medidas de seguridad adoptadas por los responsables no podrán ser menores a aquellas que mantengan para el manejo de su información y tomarán en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Las medidas de seguridad podrán ser administrativas, físicas o técnicas, y para establecer y mantener las mismas el responsable deberá considerar las siguientes acciones:

— Elaborar un inventario de datos personales y de los sistemas de tratamiento.

— Determinar las funciones y obligaciones de las personas que traten datos personales.

— Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.

— Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.

— Realizar el análisis de brecha.

— Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.

— Llevar a cabo revisiones o auditorías.

— Capacitar al personal que efectúe el tratamiento.

— Realizar un registro de los medios de almacenamiento de los datos personales.

ENCARGADOS DE TRATAMIENTO Y *CLOUD COMPUTING*

Encargados del tratamiento[104]

La figura del encargado se encuentra a su vez dentro de la figura de la remisión de datos personales, la cual es la comunicación de datos personales entre el responsable y el encargado,

---

103 Artículos 19 de la LFPDPPP y 2 fracciones V a VII, 57al 66 del RLFPDPPP.

104 Artículos 49, 50 y 53 del RLFPDPPP.

dentro o fuera del territorio mexicano. Siendo este último la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable[105].

Las remisiones nacionales e internacionales no requerirán ser informadas al titular ni contar con su consentimiento.

Ahora bien, para entender mejor la figura del encargado en conveniente analizar que es una persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Teniendo el encargado las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:

— Tratar los datos personales conforme a las instrucciones del responsable.

— Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.

— Implementar las medidas de seguridad conforme a la legislación aplicable.

— Guardar confidencialidad respecto de los datos personales tratados.

— Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable. Ello cuando no exista una previsión legal que exija la conservación de los datos personales.

— Abstenerse de transferir los datos personales salvo cuando dicha transferencia así sea determinada por el responsable o cuando lo requieran las autoridades competentes.

El encargado podrá ser considerado como responsable, cuando:

— Destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable.

— Efectúe una transferencia, incumpliendo las instrucciones del responsable y sin autorización de este último.

Cloud computing[106]

Para el tratamiento de datos personales en el cómputo en la nube o en los servicios en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:

— Tener y aplicar políticas de protección de datos personales afines a los principios y deberes de la LFPDPPP y del RLFPDPPP.

— Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.

— Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información.

— Guardar confidencialidad respecto de los datos personales.

— Contará con mecanismos para:

---

105 Artículos 3 fracción IX de la LFPDPPP y 2 fracción IX del RLFPDPPP.

106 Artículo 52 del RLFPDPPP.

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio.
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales.
c) Establecer y mantener medidas de seguridad adecuadas.
d) Garantizar la supresión de los datos personales una vez concluido el servicio.
e) Impedir el acceso a los datos personales a personas no sin privilegios de acceso, o cuando la solicitud sea fundada y motivada de autoridad competente, se informará de ese hecho al responsable.

AUTORIDAD DE CONTROL. INSCRIPCIÓN O REGISTRO DE TRATAMIENTO. PROCEDIMIENTOS. SANCIONES

Autoridad de Control

La autoridad de control es el Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI).

Procedimientos

Existen tres procedimientos relacionados con la protección de datos personales ante el IFAI, ello ya que el procedimiento de derechos ARCO se lleva a cabo ante el particular:

— Protección de derechos[107]. La solicitud de protección de datos se presentará ante el IFAI durante los 15 días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable, ello en relación a las solicitudes de derechos ARCO que se hayan efectuado.
— Si el titular no recibe respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable.
— De verificación[108]. Con el fin de vigilar el cumplimiento de las normas en la materia, el IFAI llevará a cabo este procedimiento iniciándolo de oficio o a petición de parte.
— De imposición de sanciones[109]. El cual procede en caso de que de los procedimientos de protección de derechos o de verificación, se tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de las normas en la materia.

Sanciones[110]

Las sanciones por motivo del incumplimiento de las obligaciones y disposiciones establecidos en la LFPDPPP podrán ser las siguientes:

— Apercibimiento.
— Multas que ven desde los $6,729 a los $2.1 millones de pesos, multas que podrán ser duplicables en caso de reincidencia.

---

107 Capítulos VII de la LFPDPPP y VIII del RLFPDPPP.
108 Capítulo VIII de la LFPDPPP y artículos 128 al 139 del RLFPDPPP.
109 Capítulo IX de la LFPDPPP y artículos 140 al 144 del RLFPDPPP.
110 Artículos 63 al 69 de la LFPDPPP.

Además de lo anterior también se contemplan delitos que podrán ser sancionados con prisión que podrá ir desde los 6 meses a los 5 años.

LEGISLACIÓN ESPECÍFICA

Administración pública

México tiene la particularidad de que la protección de los datos personales se divide en dos ámbitos, la protección de datos ante particulares regulados por la LFPDPPP y los que se encuentran en posesión de las autoridades, los cuales son regulados por las normas de transparencia y acceso a la información pública gubernamental, regulado a nivel Federal por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG).

Entre las principales diferencias respecto de la LFTAIPG y la LFPDPPP, se encuentran:

— Los responsables del tratamiento de los datos personales son los sujetos obligados, los cuales son las entidades gubernamentales responsables del tratamiento.

— Únicamente se contempla el consentimiento expreso. Excepto cuando el tratamiento sea necesario por razones estadísticas, científicas o de interés general; se transmitan entre sujetos obligados o entre dependencias y entidades; por orden judicial; y cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales.

— Solo se contemplan los derechos de acceso y corrección de los datos personales.

La autoridad reguladora en el caso de estos datos también es el IFAI.

Banca y seguros

Uno se los sectores más regulados es el sector bancario y financiero, en donde tenemos alrededor de 60 disposiciones aplicables, así como diversas autoridades reguladoras como son el Banco de México, la Comisión Nacional Bancaria y de Valores, la Comisión Nacional de Seguros y Fianzas, la Comisión para la Defensa de los Usuarios de Servicios Financieros, el Instituto de Protección al Ahorro Bancario y la Comisión Nacional del Sistema de Ahorro para el Retiro.

Pero en materia de datos personales, uno de los aspectos principales es el secreto bancario por medio del cual se protege la privacidad del cliente bancario (en relación con las operaciones activas, pasivas y de servicios de los bancos), fortaleciendo la confianza del público en el sistema financiero[111].

Así mismo se tiene un Registro de Usuarios que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios, de manera que las Instituciones Financieras no podrán utilizar la información de sus clientes con fines mercadotécnicos o publicitarios, así como enviar publicidad a los clientes que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el Registro.

Consumidores y usuarios[112]

En la Ley Federal Protección al Consumidor también se contempla un Registro de Usuarios, de manera que se establece el derecho de los consumidores a no ser molestados en su domicilio,

---

[111] Artículo 8 de la Ley de Protección y Defensa al Usuario de Servicios Financieros.

[112] Artículos 17, 18 y 18 bis de la Ley Federal de Protección al Consumidor.

lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad.

El consumidor también podrá exigir a proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.

Siendo así que la Procuraduría Federal de Protección al Consumidor podrá llevar, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Servicio que es gratuito.

Derechos fundamentales

La protección de datos personales se encuentra contemplada como uno de los derechos fundamentales, ya que se encuentra prevista desde el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos y en el cual se establece que: «Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros»[113].

Salud

En el caso de los datos personales relacionados con la salud, además de que su protección está garantizada por las normas de protección de datos personales sea que se encuentren en el ámbito privado o gubernamental, existe una norma que regula en específico el tratamiento de los datos e información sanitaria contenida en el expediente clínico. Dicha norma es la NORMA Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico.

MIRADA HACIA EL FUTURO

En el caso de México y a diferencia de muchos países en los cuales el tratamiento de los datos personales se regula en una sola legislación, es decir, en una sola norma se contempla la protección de los datos personales sea que se encuentren en posesión de los entes públicos o privados, en el caso de México los datos personales se encuentran regulados en dos normas distintas.

En el caso de los datos personales en posesión de particulares, la norma que los regula es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), mientras que los datos personales en posesión de las autoridades o entes públicos se encuentran regulados por las normas de transparencia, de las cuales, a nivel federal tenemos la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), sin embargo, por ser una materia concurrente también tenemos normas de transparencia en los niveles Estatal y Municipal.

Ahora bien, en relación a la protección de datos personales en posesión de los particulares, se encuentran en el Congreso de la Unión 2 propuestas de reforma:

---

[113] Segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

1. Reforma en la que se adecua el concepto de datos personales sensibles para adicionar de manera específica los datos biométricos, así como el que respecto al consentimiento tácito, se establece expresamente que en el caso de los menores de edad, el mismo nunca será tácito y para que se pueda considerar consentimiento expreso, deberá constar la autorización del padre o tutor[114].
2. Actualmente en materia de publicidad quienes desean restringir el uso de sus datos personales de manera que no sean usados para hacerles llegar publicidad, basta con que así lo manifiesten para que no se les vuelva a enviar, sin embargo, existe una iniciativa de reforma mediante la cual queda prohibido enviar información publicitaria a las personas que no manifiesten expresamente su voluntad para recibirla, lo cual actuaría prácticamente a la inversa del modelo actual[115].

Pero además de las anteriores iniciativas de reforma, también por lo que ve a la protección de datos personales en posesión de las autoridades existe una propuesta pero para la emisión de la «Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados»[116]. La cual contempla las siguientes modificaciones:

— Este proyecto de ley dimensiona la protección de datos personales de los tres niveles de gobierno, por lo que ya no existirían diversos tipos de legislaciones.

— Se separan las materias de transparencia y acceso a la información pública, ya que en las actuales normas de transparencia se incluye un capítulo relacionado con la protección de datos personales. De manera que la protección de datos esté contenida en una sola norma.

— Al unificar la protección de datos personales en posesión de autoridades en una sola norma, uno de los objetivos que se buscan es que mediante la misma se realice una distribución de competencias en los niveles Federal, Estatal y Municipal.

— El órgano garante en la materia que actualmente es el Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI), cambia su nombre a Instituto Nacional de Acceso a la Información y Protección de Datos Personales.

— Se consideran los cuatro derechos ARCO, acceso, rectificación, cancelación y oposición, ya que en las normas actuales de transparencia no se encuentra estandarizado el tomar los cuatro derechos, por lo general solo se considera el acceso y rectificación, dejando de lado sobre todo la cancelación.

— Se plantea la creación de una Plataforma Nacional de Información, la cual integrará sistemas de transparencia, acceso a la información y protección de datos.

— En términos generales, se toman muchos de los conceptos y estructuras de la LFPDPPP, tales como transferencia, encargado, tercero, tratamiento, principios, entre otros.

---

114 Cámara de Diputados, «Iniciativa que reforma los artículos 3o. y 8o. de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares», México, 2013. Tomado de http://gaceta.diputados.gob.mx/Gaceta/62/2013/abr/20130425-IX.html#Iniciativa11.

115 Cámara de diputados, «Iniciativa que reforma y adiciona diversas disposiciones de las Leyes Federal de Protección al Consumidor, de Protección y Defensa al Usuario de Servicios Financieros, y Federal de Protección de Datos Personales en Posesión de los Particulares», México, 2014. Tomado de http://gaceta.diputados.gob.mx/Gaceta/62/2014/abr/20140408-VI.html#Iniciativa2

116 Instituto Federal de Acceso a la Información Pública y Protección de Datos, «Propuesta de Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados», México.
Tomada de http://inicio.ifai.org.mx/nuevo/Propuesta%20de%20Ley%20General%20de%20PD%20PDF.pdf.

2.8 NICARAGUA

Constitución Política

Artículo 26: Toda persona tiene derecho: A su vida privada y la de su familia; A la Inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo;(…). A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información.

Por medio de la Ley 831 del 30 de Enero del 2013, Ley de Reforma y adiciones a la Ley 49, Ley de Amparo, es que en Nicaragua se incluyó el Recurso de *Habeas Data*. De conformidad al arto 5 bis; «El Recurso de *Habeas Data* se crea como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya una invasión a la privacidad personal y tenga relevancia con el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar.

El Recurso de *Habeas Data* procede a favor de toda persona para saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales y su publicidad indebida». Con esta reforma es que se procede al tratamiento procesal de protección de los datos personales en sede jurisdiccional por primera vez en Nicaragua. Se plasma el derecho ciudadano de acudir ante la sala constitucional de la Corte Suprema de Justicia a interponer el recurso de *Habeas Data* cuando consideren que su derecho a la privacidad ha sido vulnerado o se ha hecho un uso incorrecto de sus datos personales, de igual forma se abre la puerta al resarcimiento económico por daños infringidos cuando se vulneren los mencionados derechos.

Un año antes a esta reforma, fue aprobado en el seno de la Asamblea Nacional la Ley de Protección de Datos Personales, donde se establece una instancia administrativa para recurrir cuando el ciudadano considere que han sido lesionados sus derechos a la intimidad, privacidad y autodeterminación informativa. Dentro de esta normativa no se estableció el recurso de *Habeas Data* por contener derechos de rango constitucional y se consideró ampliar la Ley de Amparo incluyendo esta figura, elevándola a rango constitucional.

En el momento de la aprobación de la reforma a la ley de Amparo, hubo un sector de juristas, especialmente constitucionalistas que mostraron inconformidad con la reforma por algunas de las siguientes razones:

Aunque la reforma contiene ventajas, algunos advierten sobre «ciertas debilidades» en la nueva legislación en materia de amparo a través del denominado recurso de *habeas data* o de protección de datos personales, por cuanto puede tender atentar contra la libertad de prensa, ya que abarca las entidades privadas.

De igual manera, la reforma contempla que cabe el recurso de *habeas data* contra cualquier persona u organización que compile información sobre cualquier ciudadano e incluso es puede ser obligado a destruirla. Se ejemplifico que sí un periodista realiza una investigación sobre cualquier funcionario público, éste podría hacer uso del recurso de *habeas data,* y si la sala Constitucional de la Corte Suprema de Justicia falla a su favor, podría obligar al periodista a no publicar esa información e, incluso, a destruirla.

Otros por el contrario, defendieron el avance en materia de protección de datos que logró con la reforma a la ley de amparo que dio poder a la Ley 787, ley de protección de datos

personales, que entró en vigencia en marzo de 2012. Algunos juristas[117] como Asunción Moreno, señalan:

«De tal forma que el tema debe verse como una interrelación entre el derecho a la privacidad, la protección de datos y el *habeas data* como una forma de ejercer nuestro derecho a saber.»

«Esta ley amplía la protección de nuestros datos personales no solo al ámbito público, sino también privado. Hay que recordar que sectores como los bancos, empresas telefónicas y comerciales, etcétera, recopilan datos personales y en ocasiones no nos consultan o no nos informan con qué finalidad.»

«… viene a ser una garantía para que todas las personas podamos saber quién, cuándo, dónde y bajo qué circunstancias se ha tenido acceso a nuestros datos personales…»

«… se trata de la protección de la persona frente al tratamiento de sus datos personales, y constituye una forma de complementar la tutela que ya había recibido por medio del precepto constitucional que contempla la protección de la privacidad…»

«… Se trata de una regulación propia de la tercera generación de derechos humanos, dirigida a alcanzar para el individuo medios para oponerse a los potenciales riesgos y peligros a los que se enfrenta en la sociedad tecnológica. Por ello, no creo que afecte la libertad de expresión, ni la de información mucho menos la libertad de prensa.»

La evolución legislativa del *habeas data* en el contexto nicaragüense se ubica en diferentes momentos según señala el autor Omar A. García[118], al decir:

«La Ley de Amparo vigente es de 1988 y ha sido reformada en 1995, 2008 y 2013. Es una Ley Constitucional que tiene un tratamiento especial dentro del sistema de fuentes de la Constitución.

La reforma de 2013, introduce, entre otras cosas, la regulación procesal jurisdiccional del Recurso de *Habeas Data*. El reconocimiento a la protección de datos personales había sido creado como derecho en las reformas a la Constitución en 1995. Particularmente, el artículo 26 numeral 4) reconoció la existencia de ese derecho (derecho a la autodeterminación informativa).

El mecanismo jurisdiccional de protección de ese derecho fue establecido en la reforma de 2013. Sin embargo, cabe destacar que entre 1995 y el 2013, el ordenamiento jurídico y la jurisprudencia de la Corte Suprema de Justicia, tímidamente fueron regulando y abordando dicho derecho e inclusive se definió normativamente el mecanismo de protección *Habeas Data*. De igual forma, es un tema que poco a poco ha ido despertando interés y existen algunos trabajos monográficos como los de Pineda Quinteros y Obando Quezada que explican la importancia de contar con un mecanismo específico de protección de Derechos a la autodeterminación informativa más allá de la protección de derechos mediante el Recurso de Amparo y del Recurso de Exhibición Personal.

Ahora bien, el 5 de marzo de 2008, se presentó una iniciativa de reforma a la Ley de Amparo para regular el *Habeas Data* en sede jurisdiccional. Cabe destacar, que en 2012, en la Ley de Protección de Datos Personales se creó el mecanismo de protección procesal en sede

---

117 Publicado en http://m.end.com.ni/noticias?idarticulo=276486.

118 Asesor legislativo en la Asamblea Nacional, Comisión de Justicia y Asuntos Jurídicos, Catedrático del Instituto Nicaragüense de Estudios Jurídicos (INEJ), La importancia de la reforma de 2013 a la Ley de Amparo, artículo Publicado en la Revista Parlamentaria MONÉXICO. Edición n.º 19. IV Etapa. Febrero-marzo 2013. Págs. 8-11.

administrativa (art. 47 al 51) y se siguió el criterio de la Sala de lo Constitucional citado en la Sentencia n.º 60 de 18 de enero de 2007, en tal sentido, el artículo 52 de la Ley de Protección de Datos Personales señaló que mientras no existiera un mecanismo procesal jurisdiccional específico, los derechos a la autodeterminación informativa se protegerían mediante el Recurso de Amparo. En abril de 2012, se creó una Comisión Especial de Carácter Constitucional para dictaminar el Proyecto de reforma presentado en 2008.

La reforma a la Ley de Amparo se produjo mediante Ley n.º 831. Publicada en La Gaceta Diario Oficial n.º 29 de 14 de febrero de 2013».

Como hemos referido anteriormente, el recurso de *habeas data,* tiene como base constitucional el artículo 26, numerales 1, 3 y 4 de la constitución política de la República de Nicaragua, por lo que puede interponer el recurso todo aquel que desee:

1. Acceder a información personal que se encuentre en poder de cualquier entidad pública y privada de la que generen, produzcan, procesen o posean información personal, en expedientes, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier documento que la administración pública o las entidades privadas tengan en su poder.

2. Exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación, y actualización, de datos personales sensibles independientemente que sean físicos o electrónicos almacenados en ficheros de datos, o registro de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros, cuando se presuma la falsedad, inexactitud, desactualización, omisión total o parcial o la ilicitud de la información de que se trate.

3. Exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización de cualquier publicidad de datos personales sensibles que lesionen los derechos constitucionales.

Este podrá ser interpuesto por el afectado, sus tutores y los sucesores de las personas naturales o por intermedio de apoderado. Cuando el recurso sea presentado por personas jurídicas, deberá ser interpuesto por sus representantes legales, o apoderados designados para tales efectos.

Para interponer el recurso de *habeas data* se requiere haber agotado la vía administrativa contemplada en la ley de protección de datos personales, en la vía administrativa procede el silencio administrativo cuando pasan 30 días y la autoridad administrativa no ha emitido resolución alguna sobre el reclamo interpuesto.

Este recurso se dirige contra los responsables y cualquier otra persona que hubiere hecho uso indebido de ficheros de datos públicos y privados. Los responsables de los ficheros de datos no puedan alegar confidencialidad de la información que se les requiera, salvo en el caso de que se afecten fuentes de información periodística. Cuando la confidencialidad se alegue en los casos de excepción previstos en la ley, la sala de lo constitucional de la corte suprema de justicia puede tomar conocimiento personal y directo de los datos, asegurando el mantenimiento de su confidencialidad.

Una vez determinado por la sala constitucional de la corte suprema de justicia que se produjo lesión a los derechos del titular de los datos, dictará las medidas que estime pertinentes para el cumplimiento del fallo.

Por último, podemos decir que en materia de protección de datos, la institucionalización del *habeas data,* como un mecanismo de tutela de derechos constitucionales, ha sido un gran avance que permitirá incursionar en la economía digital con una protección adecuada para el ciudadano.

Las constituciones políticas obedecen a cambios sociales y en el contexto nicaragüense, donde la incursión de internet en la población es la menor en la región, hace que pensemos en abrir las puertas a estos cambios sociales y tecnológicos, obligándonos a reestructurar nuestra legislación en pro de ser más competitivos en el mercado de las empresas digitales.

Nicaragua hoy en día no cuenta con una ley de comercio electrónico, pero ya cuenta con leyes de firma digital, protección de datos, *habeas data* y normativas dispersas, tanto en tratados vinculantes y normas internas, lo que nos hace ver que hay una economía digital pujante y pendiente de explotar, donde los datos personales ya comienzan a fluir como un bien de alto valor comercial entre los sujetos de comercio y es por ello que el Estado como soberano y tutelar de las relaciones y derechos de los ciudadanos debe tener especial atención en frenar condiciones de desventaja entre las partes.

2.9 PERÚ

Constitución Política

> Artículo 2: Toda persona tiene derecho a: 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal (…). Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

Hoy todos generamos información a sabiendas o no, en especial la información personal la que se refiere a uno mismo, la cual tiene un valor comercial, y no solo la que se refiere a mi patrimonio sino también la que puede indicar quien soy yo o lo que los demás sepan de mí aunque ni yo sepa qué tipo de información puedan obtener de lo que hago o dejo de hacer.

En el Perú, esta data denominada dato personal, ahora debe ser resguardada, ya no solo a mérito de la protección constitucional reconocida en el artículo 2 inciso 6 en la Constitución política de 1093, por la garantía constitucional *Habeas data* dispuesta en la Constitución y en el Código Procesal Constitucional, sino también por lo dispuesto en la Ley n.º 29733 – Ley de Protección de datos personales (en adelante, Ley PDP) y en el Decreto Supremo n.º 0013-2013-JUS-Reglamento de la Ley n.º 29733.

En la Ley PDP se delimita el ámbito de aplicación de esta, cuyo Reglamento la ha complementado, no aplicándose las reglas establecidas en estos dos textos legales a los datos personales destinados o contenidos a un banco de datos personales de uso privado o familiar, o en caso de la administración pública si el banco tiene por objeto la defensa nacional, la seguridad pública y el desarrollo en materia penal para la investigación y represión del delito.

El objeto de la protección de datos no es la salvaguardia jurídica de estos sino de las personas que son titulares de estos, además que el titular de los datos jamás pierde la titularidad de los datos, no importa si es que ellos no lo originaron de manera directa, si lo cedieron, ya que la cesión solo es para el tratamiento de este, solo en algunos casos se podrá limitar su acceso a l titular de datos como en casos de seguridad nacional. Según la Ley peruana la limitación al ejercicio solo puede ser establecida por ley y debe estar justificado en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos.

BIEN JURÍDICO PROTEGIDO: DEFINICIÓN DE DATO DE CARÁCTER PERSONAL

La Ley PDP establece que los datos personales son toda aquella información que nos identifica o nos pueda hacer identificable a través de medios que puedan ser razonablemente utilizados, así tenemos no solo nuestros nombres y apellidos, los datos contenidos en los documentos de identidad como el DNI, el pasaporte, licencia de conducir, entre otros, los datos contenidos en una solicitud para identificar al solicitante, el sexo.

El Reglamento de la Ley PDP, complementa a lo mandado en la Ley de Protección de datos personales, señalando que es aquella información numérica (edad, número de DNI), alfabética (nombres, apellidos, sobrenombre), gráfica (firmas que distingan nombres), fotográfica (fotos de perfil, retratos), acústica (grabaciones de voz), sobre hábitos personales (tipos de consumo o compras). Es decir, es toda data que nos identifica y distingue como individuo.

La Ley manda una especial atención y salvaguarda a un determinado dato personal al que denomina dato sensible. Este tipo de dato, a nivel doctrinal es aquel cuyo conocimiento sin consentimiento del titular de este dato puede generar un daño irreparable a la persona, provocar discriminación, son todos aquellos que son parte de la esfera más íntima y reservada de un individuo.

La Ley PDP contempla como datos sensibles a los datos biométricos que por sí mismos puedan identificar al titular, aquello que denoten el origen racial o étnico, ingresos económicos, opiniones y convicciones: políticas, religiosas, filosóficas o morales, afiliación sindical, información relacionada a la salud física o mental (salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética) que afecten su intimidad, información relacionada a la vida sexual. El Reglamento de la Ley incluye a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima.

Todos estos datos personales pueden estar organizados o no en un banco de datos personales, esta organización puede ser automatizada o no, así podemos considerar un banco de datos personales desde el tarjetero organizado encima de la secretaria de una entidad hasta los registros en soportes magnéticos de los clientes de una gran empresa.

INFORMACIÓN Y CONSENTIMIENTO. OBLIGACIÓN DE TRANSPARENCIA

Toda aquella actividad o procedimiento de cualquier naturaleza que se realice sobre el dato personal, sea desde su recopilación, registro, organización, extracción, consulta, difusión, interconexión con otros datos, entre otras forma de procesamientos nombrados en el artículo 2 numeral 17 de la Ley PDP, se le denominará «tratamiento de datos personales». Son estos tipos de procedimientos, los cuales serán el eje temático y casi central de toda la regulación de la Ley PDP y su Reglamento para advertir que un dato personal está siendo usado de manera correcta según previsiones de las normas legales. Las condiciones del tratamiento son:

— El consentimiento debe ser «libre», ningún vicio de la voluntad previsto en el código civil peruano deberá haber estado presente en el momento de dar el consentimiento. No se podrá sujetar el consentimiento al otorgamiento de algún beneficio para el caso de menores de edad.

— Debe ser «previo», es decir anterior a la recopilación del dato personal.

— Ser «expreso e Inequívoco», que no de dudas de su otorgamiento. Puede ser un expreso oral o escrito, por cualquier medio o soporte que pueda dar una constancia fidedigna que el titular del dato dio su consentimiento de forma clara y que pueda ser probada por el titular o encargado del banco de datos personales.

— Además de ser «informado», al titular de los datos personales se le debe de comunicar de forma clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos de lo siguiente sobre la identidad de los responsables del tratamiento del dato, un domicilio donde ejercer sus derechos, las finalidades del tratamiento, modo de ejercicio de sus derechos, quienes accederán a su información y para qué fines, y solicitar consentimiento si se realizará una transferencia internacional de protección de datos personales.

El consentimiento otorgado por el titular de los datos, puede ser revocado por el mismo en cualquier momento, observando al efecto los mismos requisitos que con ocasión de su otorgamiento.

EXCEPCIONES DE CONSENTIMIENTO

La Ley prevé excepciones para requerir el consentimiento del titular de los datos personales, las entidades privadas no requerirán este requisito cuando:

— Los datos personales están o serán contenidos en fuentes accesibles por el público.

— Los datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley (los datos recopilados por las centrales de riesgo[119]).

— Cuando medie norma para la promoción de la competencia en los mercados regulados referida a la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.

— Los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte.

— Los datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.

— Los datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública.

— Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros.

— Si se hubiera aplicado un procedimiento de anonimización o disociación.

— Si el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales.

DATOS ESPECIALMENTE PROTEGIDOS Y OTROS TRATAMIENTOS INVASIVOS

La Ley ha reservado el tratamiento de los datos personales relativos a la comisión de infracciones penales o administrativas solo a las entidades públicas excluyéndola del ámbito de las entidades privadas. Estos datos personales solo podrán ser tratados por una entidad privada si existiera un convenio de encargo de gestión conforme a la Ley n.º 27444 Ley del Procedimiento Administrativo General.

---

[119] Ley 27489, Ley que Regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información.

La información de los antecedentes penales, judiciales, policiales y administrativos; luego de su cancelación no pueden ser suministrados salvo que sean requeridos por el Poder Judicial o el Ministerio Público, conforme a lo requerido por ley.

CESIONES DE DATOS

Si una entidad privada (sea mediante el titular o el encargado del banco de datos personales) desea transferir los datos personales que tiene bajo su cargo hacia otro país, el país destinatario deberá tener niveles de protección adecuados exigidos por la Ley, es decir que dicho país tenga legislación de protección de datos personales al menos equiparable al previsto por la ley peruana o cumpla con los estándares internacionales en la materia.

Si el país destinatario no cuenta con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe garantizar que el tratamiento de los datos personales se efectuará conforme a lo dispuesto por la Ley PDP. Se debe hacer con respeto de los principios rectores establecidos en la Ley, de las medidas técnicas de seguridad y confidencialidad, todo ello en concordancia según la categoría de dato que se trate, puesto que un dato sensible requerirá mayor cautela que otro dato personal.

No se requerirá esta garantía en los siguientes casos: acuerdos en el marco de tratados internacionales sobre la materia en los cuales la República del Perú sea parte, cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, cuando se trate de transferencias bancarias o bursátiles, cuando el flujo transfronterizo de datos personales se realice para la protección, prevención, diagnóstico o tratamiento médico o quirúrgico de su titular; o cuando sea necesario para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados y cuando el titular de los datos personales haya dado su consentimiento.

CALIDAD DE LOS DATOS

Los principios rectores de la Ley PDP son referidos a las garantías al tratamiento de los datos personales para hacerlos idóneos y seguros, son conocidos también en doctrina como principios de calidad de datos. Todos estos principios rectores servirán como criterio de interpretación para resolver aplicaciones de la Ley PDP que los expone así. Entre ellos, se e encuentra el principio de calidad el cual exige que los datos sean exactos y estén actualizados (o puestos al día) de forma que respondan con veracidad a la situación del afectado a fin de garantizar y proteger la calidad de la información sometida a tratamiento. Cuando los datos sean recogidos de manera directa del titular de ellos se podrá asumir que estos son exactos.

HABEAS DATA Y DERECHOS ARCO

En caso el titular del datos personal ante un caso de vulneración del derecho a la protección de datos personales desee iniciar una medida de protección sobre sus datos, puede accionar cualquiera de la dos vías contempladas en la legislación peruana: la acción constitucional del *Habeas Data* (desarrollada en los artículo 61 y ss. del Código Procesal Constitucional) o un procedimiento trilateral de tutela ante la Autoridad Nacional de Protección de Datos Personales. Para ambas vías se condiciona que previamente el titular del dato haya reclamado sus derechos ante la entidad respectiva encargada del banco de datos.

El derecho a la protección de datos es un derecho genérico que se sustenta de otros derechos específicos propios del derecho del titular de los datos, tales como: el derecho a acceder, el derecho a conocer, el derecho a rectificar, derecho a la oposición y derecho al tratamiento objetivo del dato.

Derecho a la información

Este derecho reside en saber la existencia de los bancos de datos que contienen datos individuales.

Derecho de acceso a los datos

El derecho de acceso a los datos permite a los titulares de los datos indagar el contenido de la información contenida sobre ellos en un banco de datos, así como el objeto y finalidad de su existencia, la identidad del responsable o titular del banco de datos personales, y cuál es el ámbito de la circulación de los datos (nacional y/o internacional).

Este derecho no solo permitirá el acceso a los datos sino también permitirá el control, verificar la verosimilitud de estos, verificar si son datos aportados de manera voluntaria, y en caso contrario de que no haya mediado el consentimiento verificar la licitud de la forma de obtención de estos. En caso de irregularidad de la obtención se podrá demandar la supresión de estos.

Derechos de rectificación y cancelación

Es posible que al acceder a sus datos, el titular de ellos compruebe que estos sean incorrectos, inexactos u obsoletos (que ya no correspondan a la realidad actual).

Para la rectificación de estos datos que no pertenecen a la realidad, ocasionan o pueden ocasionar daños al afectado, se utiliza el *habeas data* (en la mayoría de las legislaciones) como el mecanismo idóneo para alcanzar esta finalidad, en nuestra legislación la Ley PDP y su Reglamento nos da un nuevo mecanismo administrativo para ello.

El ejercicio del derecho a rectificar tiene como meta a los datos personales «reales», y no a meros juicios de valor o comentarios fundados en aquéllos[120]. Es decir, en datos objetivos que se han probado en manera fehaciente.

La rectificación debe proceder cuando los datos sean incorrectos o no se ajusten a los principios básicos de protección de datos[121] como el de principio de calidad. Este derecho a rectificar es independiente si el error fue a causa del dolo o culpa del titular del registro.

El derecho a rectificar no debe ser confundido al de la réplica que surge cuando se trata de ataque malicioso contra la honra o contra aspectos fundamentales de la persona, o contra sus convicciones personales.

Derecho de oposición

Esta intervención del afectado es una facultad activa para que el mismo pueda exigir la oposición de la inscripción de sus datos o que estos sean retirados o borrados del banco de datos personales.

Derecho al tratamiento objetivo de datos personales

Si a un dato personal lo enriquecemos con otro tipo de data que nos pueda identificar o decir más sobre un individuo, ayudando a hacer un juicio de valor sobre la persona; este

---

120 EKMEKDJIAN, M. Á. y PIZZOLO, C.: Habeas data: *El Derecho a La Intimidad Frente a La Revolución Informática,* 1.ª ed, Ediciones Desalma, Buenos Aires, 1998, p. 8.

121 Según el Convenio n.º 108 del Consejo, de 28 de enero de 1981, de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal.

derecho brinda a que el titular del dato no sea sometido a este acto de evaluación sin previo consentimiento y/o conocimiento del titular del dato personal si ello afecta de manera significativa a la persona o produce efectos legales sobre ella.

Se exceptuará si esto ocurre dentro del marco de una negociación o contrato, o en los casos de contratación en una entidad pública. Esto no limitara el derecho de la persona a defender su punto de vista. Además si el tratamiento se realiza en un proceso de toma de decisiones sin participación del titular del dato, se le deberá avisar de dicho tratamiento.

Medidas de seguridad

Además del consentimiento del titular de los datos, la ley prevé otras dos condiciones para el tratamiento de los datos personales, los deberes de seguridad y confidencialidad.

Seguridad

El titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado. La Autoridad Nacional de Protección de Datos Personales establecerá dichas medidas, salvo la existencia de disposiciones especiales contenidas en otras leyes.

Actualmente existe la Directiva de Seguridad de la Información para banco que administren datos personales en la cual se establecen los 5 niveles de protección según las características del banco de datos, en la Directiva se establecen medidas de seguridad organizacionales, técnicas y legales, estas medidas son a modo de recomendación según lo indicado en el texto de la Directiva.

Confidencialidad

El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aún después de finalizadas las relaciones con el titular del banco de datos personales, sin perjuicio del derecho a guardar el secreto profesional.

ENCARGADOS DE TRATAMIENTO Y *CLOUD COMPUTING*

A la persona o entidad que realizara el tratamiento de datos personales por encargo del titular del banco de datos, se le denominará «encargado del banco de datos personales». Estos personajes estarán obligados al cumplimiento de la Ley PDP siempre y cuando el banco de datos personales esté dentro del ámbito de la Ley PDP, no se necesita que el establecimiento principal de la entidad esté en Perú, el Reglamento solo exige que si cualquier aspecto del tratamiento aun su solo almacenamiento, entonces el titular del banco de datos o en su encargado estarán dentro del ámbito territorial de la Ley PDP y su Reglamento.

Respecto a los servicios desarrollados en la Nube o *Cloud Computing* estos se encuentran regulados en el Reglamento de la Ley PDP a través de la denominación «Tratamiento de los datos personales por medios tecnológicos tercerizados» en el cual se establecen obligaciones de transparencia del tratamiento de la información. El tratamiento de datos personales por medios tecnológicos tercerizados, sea completo o parcial, podrá ser contratado por el responsable del

tratamiento de datos personales siempre y cuando para la ejecución de aquel se garantice el cumplimiento de lo establecido en la Ley PDP y en su reglamento.

AUTORIDAD DE CONTROL. INSCRIPCIÓN O REGISTRO DE TRATAMIENTO. PROCEDIMIENTOS. SANCIONES

El Ministerio de Justicia y Derechos Humanos es la Autoridad Nacional de Protección de Datos Personales, la cual debe realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la Ley PDP y de su reglamento, para ello goza de una potestad sancionadora.

La Autoridad Nacional de Protección de Datos personales tiene entre sus principales funciones el de velar por el cumplimiento de la Ley PDP, en caso de infracción a la Ley es el Director de las Sanciones de la Autoridad quien instruye y resuelve en primera instancia y el Director General de Protección de Datos Personales resolverá en segunda y última instancia el procedimiento sancionador. Este procedimiento será promovido siempre de oficio, que puede obedecer a una denuncia de parte o por decisión motivada del Director de la Autoridad. Se han establecido infracciones leves, graves y muy graves. Las sanciones pueden ser pecuniarias, la Autoridad puede mandar medidas correctivas e inclusos medidas cautelares en caso de ser necesario.

Respecto a inscripción de los bancos de datos personales, estos deberán ser inscritos en el Registro Nacional de Protección de Datos Personales (actualmente mediante previo pago ante la Autoridad), registro que es de carácter público. En el Registro Nacional también se inscribirán los códigos de conducta, las sanciones, medidas cautelares o coercitivas impuestas por la Autoridad y comunicaciones del flujo transfronterizo de los datos.

Administración pública

El Reglamento de la Ley PDP establece que este se aplicará a toda modalidad de tratamiento de datos personales, ya sea efectuado por entidades públicas independientemente del soporte en el que se encuentren.

El reglamento de la Ley PDP aclara que no se aplicará la normativa de protección de datos personales cuando los datos solo tengan por objeto para la defensa nacional, seguridad pública y desarrollo de actividades e materia penal para la investigación y represión del delito.

Además vemos las salvedades para la estricta ejecución de la interoperabilidad en el artículo 11.º del Reglamento de la Ley y en la Disposición Complementaria Final Primera.

Se considerara como fuente accesible al público los bancos de datos de las entidades de la Administración Pública, en relación a la información que deba ser entregada en aplicación de la Ley n.º 27806, Ley de Transparencia y Acceso a la Información Pública.

Algunos casos previstos para la cooperación internacional, han sido previstos para la transferencia internacional de datos sin que sea necesario el consentimiento y cumplimiento de las exigencias de dispuestas para el flujo transfronterizo, así tenemos: acuerdos en el marco de tratados internacionales y Perú sea parte, cooperación judicial internacional, y Cooperación internacional entre organismos de inteligencia para la lucha contra el i) terrorismo, ii) tráfico ilícito de drogas, iii) lavado de activos, iv) corrupción, v)trata de personas y vi) otras formas de criminalidad organizada.

Por otro lado, se ha publicado la Resolución Directoral n.º 060-2014-JUS/DGPDP, en el cual el Ministerio de Justicia mediante la Dirección General de Protección de Datos Personales

aprueba la «Directiva n.º 001-2014-JUS/DGPDP sobre protección de datos personales en el marco de procedimientos para la construcción, administración, sistematización y actualización de bases de datos personales vinculados con programas sociales y subsidios que administran el Estado».

LEGISLACIÓN ESPECIALIZADA EN OTRAS ÁREAS

En la Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, se establecen obligaciones de verificación y veracidad de la identidad de las personas, así como el resguardo de la información de estas que estén bajo su responsabilidad.

El Código del Consumidor en su artículo 42 «Información sobre consumidores en centrales privadas de riesgo» establece un derecho de acceso y conocimiento de los datos personales que traten los buró de créditos o centrales de riesgo así todo consumidor tiene derecho a conocer los datos, el contenido y las anotaciones de su historial crediticio registrado en las centrales de riesgo en forma gratuita mediante la visualización en pantalla y cuando lo considere necesario. Asimismo, las centrales de riesgo están en la obligación de salvaguardar la información personal de los consumidores bajo responsabilidad y a que la información que sea pública responda a la situación real del titular de la información en determinado momento (principio de calidad).

La Ley PDP tiene como su objeto la protección de Datos Personales, el cual está reconocido en la Constitución Política en el artículo 2.º inciso 6 como un derecho constitucional, el cual está garantizado con la acción constitucional del *Habeas Data*.

La STC del EXP. n.º 666-96-HD/TC, especificó los alcances del inciso 6) del artículo 2.º de la Constitución, considerando que este inciso también se aplica para la actualización, rectificación, cancelación y adición de datos y no solo a la posibilidad de acceder a los registros como se podía deducir de una interpretación literal del inciso en mención.

En el derecho constitucional al secreto de las telecomunicaciones reconocido en el artículo 2.º inciso 10 de la Constitución Política se prohíbe además toda injerencia arbitraria o abusiva en la vida privada de las personas, específicamente, en sus comunicaciones, independientemente de su contenido.

Respecto a los datos de salud, la Ley PDP establece que no se necesitará consentimiento en los datos relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado por establecimientos de salud o por profesionales de ciencias de la salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.

La Ley n.º 30024, Ley que crea el Registro Nacional de Historias Clínicas Electrónicas, se establece el derecho del paciente de subsanar los datos registrados en la historia electrónica si estos estuviesen incompletos o errados.

Se exige la trazabilidad y confidencialidad en el Registro, que la Ley de protección de datos personales exige dichas medidas de seguridad a los bancos de datos automatizados como lo será el Registro Electrónico.

La Ley de Registro de Historias clínicas determina que el paciente o su representante otorgarán la autorización para que los profesionales de salud, esta autorización se realizará de manera expresa. Aunque la Ley no ha desarrollado o tratado a que se refiere con «expresa», hecho que tal vez se trate en su Reglamento, se debería tener en cuenta lo determinado ya por la Ley de protección de datos personales, es decir por escrito, firma digital u otro medio de autenticación de la identidad de la persona.

La Resolución Ministerial n.º 111-2009-MTC/03 es la «Norma que establece medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones y la protección de datos personales, y regula las acciones de supervisión y control a cargo del Ministerio de Transporte y Comunicaciones», mediante la cual se establecen los supuesto en los cuales se atenta contra la protección de la información personal relativa a los abonados o usuario cuando esta es entregada a terceros cuando la ley no prevea excepciones para ello.

Según lo dispuesto en el artículo 15B de la Ley n.º 27806, Ley de Transparencia y Acceso a la Información Pública y en el artículo 17.5 del Texto Único Ordenados de esta Ley de Transparencia y Acceso a la Información Pública, se establece a la información confidencial (entre ella la información que invada la privacidad de un ciudadano) como excepción para entregar data por parte del estado, respeto y competencia debida a la especialización de esta Ley en la información de acceso pública. La Ley PDP en su Disposición Complementaria Final Octava, para el caso de la definición de datos sensibles se establecerá lo dispuesto en la Ley de Transparencia en su ámbito y no aplicar la estipulada en la Ley PDP. Todo en un marco de respeto a la transparencia y acceso a la información pública.

2.10 PORTUGAL

Constitución de la República Portuguesa

Artículo 35: 1. Derechos de los ciudadanos. 2. La ley define el concepto de datos personales, y las condiciones aplicables a su tratamiento automatizado, conexión, transmisión y utilización, y garantiza su protección por medio de un órgano administrativo independiente. 3. Límites utilización de la informática. 4. Prohibición Acceso a los datos personales de terceros, salvo en casos excepcionales previstos por la ley. 5. Prohibida la atribución de un número nacional único a los ciudadanos. 6. Acceso libre general garantizado a las redes informáticas para uso público, definiendo la ley el régimen aplicable a los flujos transfronterizos de datos y las formas apropiadas de protección de datos personales. 7. Protección datos personales mantenidos en ficheros manuales.

Em Portugal (Portugal Continental, Açores e Madeira), a Lei de Proteção de Dados Pessoais (LPDP) atualmente em vigor é a Lei n.º 67/98, publicada em de 26 de Outubro de 1998, a qual procedeu à transposição para a ordem jurídica portuguesa da Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

A Lei de Proteção de Dados Pessoais entrou em vigor a 27 de Outubro de 1998 e revogou expressamente a anterior Lei Proteção de Dados Pessoais face à Informática, a Lei n.º 10/91 publicada em 29 de Abril de 1991.

Do ponto de vista da organização sistemática a atual Lei de Proteção de Dados Pessoais encontra-se dividida e organizada em 7 Capítulos: Disposições gerais; Tratamento de dados pessoais; Transferência de dados pessoais; Comissão Nacional de Proteção de Dados; Códigos de conduta; Tutela administrativa e jurisdicional; Disposições finais.

A autoridade nacional de supervisão é a Comissão Nacional de Proteção de Dados (CNPD), cuja composição, natureza, atribuições e competências se encontram definidas no Capítulo IV da LPDP (artigos 21.º a 26.º).

No que diz respeito à proteção da privacidade e dos dados pessoais vigora em Portugal, a par da Lei de Proteção de Dados Pessoais, a Lei n.º 41/2004, publicada em 18 de Agosto

de 2004, para o sector específico das comunicações eletrónicas, que transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas), com a redação conferida pela Lei n.º 46/2012, de 29 de agosto.

DEFINIÇÃO DE DADOS PESSOAIS

A Constituição da República Portuguesa (CRP) de 1976 foi uma Constituição inovadora e pioneira no que diz respeito à proteção da privacidade e dos dados pessoais, ao consagrar o Direito Fundamental à proteção de proteção dos dados pessoais.

O art. 35.º (utilização da informática) remete para lei ordinária a definição do conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente (n.º 2).

Consagra de forma expressa o direito de acesso dos titulares, bem como os direitos de retificação e atualização, e ainda o direito a conhecer a finalidade do tratamento (n.º 1).

Proíbe expressamente o tratamento de dados sensíveis: convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação (n.º3).

Só é autorizado o acesso de terceiros a dados pessoais, nos casos excecionais previstos na lei.

Para efeitos da Lei de Proteção de Dados Pessoais (LPDP), Lei n.º 67/98, publicada em 26 de Outubro de 1998, que procedeu à transposição para a ordem jurídica portuguesa da Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, entende-se por «Dados pessoais»: qualquer informação, de qualquer natureza, independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»).

É considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social, cfr. art.º 3.º, a) LPDP.

O conceito de dado pessoal é extremamente amplo, sendo largamente maioritário na doutrina e da jurisprudência portuguesa o entendimento que considera o IP (Internet Protocol) um dado pessoal. Pelo que a sua obtenção por terceiros só é possível no âmbito de uma ação judicial, dentro de apertados requisitos e apenas mediante despacho de juiz, cfr. art.º 126º, n.º 3 (Métodos proibidos de prova), art.º 187º e 189, n.º 2 (escutas telefónicas e extensão) do Código de Processo Penal.

INFORMAÇÃO E CONSENTIMENTO. DEVER DE TRANSPARÊNCIA

De acordo com o Principio da Legitimidade, o tratamento de dados pessoais só pode ser efetuado se: o titular tiver dado de forma inequívoca o seu consentimento (manifestação de vontade, livre, específica e informada), cfr. artigos 3.º, h) e 6.º LPDP; ou então, nos casos em que o tratamento for necessário para: execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato; cumprimento de obrigação legal a que o responsável pelo tratamento; proteção de interesses vitais do titular dos dados, se física ou legalmente incapaz; execução de uma missão de interesse público do responsável pelo

tratamento; prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados, cfr. art.º 6.º LPDP.

Quando recolher dados pessoais diretamente do seu titular, o responsável pelo tratamento deve prestar as seguintes informações: identidade do responsável; finalidades do tratamento; os destinatários ou categorias de destinatários dos dados; o carácter obrigatório ou facultativo da resposta e consequências se não responder; a existência e condições do direito de acesso e de retificação, cfr. art.º 10.º da LPDP.

DATOS ESPECIALMENTE PROTEGIDOS Y OTROS TRATAMIENTOS INVASIVOS

Em cumprimento da proibição constitucional (cfr. art.º 35.º, n.º 2 CRP), a Lei Proteção de Dados Pessoais estabelece o princípio da proibição de tratamento de dados sensíveis: convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos, cfr. art.º 7.º LPDP.

O tratamento destes dados pessoais está sujeito a prévia autorização da Comissão Nacional de Proteção de Dados (CNPD), além dos casos em que é excecionalmente autorizado por lei, quando por motivos de interesse público importante for indispensável ao exercício das atribuições legais do responsável ou quando o titular dos dados tiver dado o seu consentimento expresso, em ambos os casos com garantias de não discriminação, cfr. art.º 28.º, n.º 1, a) (controlo prévio) LPDP.

O tratamento é ainda permitido: se for necessário para proteger interesses vitais do titular e este estiver física ou legalmente incapaz de dar o seu consentimento; com o consentimento do titular, por membros de fundação, associação ou organismo sem fins lucrativos de carácter político, filosófico, religioso ou sindical, no âmbito das suas atividades; respeitar a dados manifestamente tornados públicos pelo seu titular, desde que se possa legitimamente deduzir das suas declarações o consentimento; se necessário à declaração, exercício ou defesa de um direito em processo judicial e for efetuado exclusivamente com essa finalidade.

No que diz especificamente respeito a tratamento dos dados referentes à saúde e à vida sexual, incluindo os dados genéticos, é permitido apenas se for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento seja efetuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional.

Em qualquer caso o tratamento de dados sensíveis obriga sempre a especiais medidas de segurança: controlo da entrada nas instalações; controlo dos suportes de dados; controlo da inserção; controlo da utilização; controlo de acesso; controlo da transmissão; controlo da introdução; controlo do transporte; separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos, dos restantes dados pessoais, e nalguns casos —a determinar pela CNPD— a circulação em rede com transmissão cifrada, cfr. art.º 15.º LPDP.

Por outro lado, no que diz respeito à criação de perfis (profiling) a Lei de Proteção de Dados Pessoais dispõe que qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento, cfr. artigo 13.º LPDP.

TRANSFERÊNCIAS DE DADOS

Considera-se terceiro: a pessoa, autoridade pública ou qualquer outro organismo que, não sendo o titular dos dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratante, esteja habilitado a tratar os dados, cfr. art.º 3.º, f) LPDP.

A cessão de dados a terceiros só é permitida com o consentimento do titular, o qual para ser uma «manifestação de vontade, livre, específica e informada», cfr. art.º 3.º, h) deve ser comunicada ao titular previamente à obtenção do seu consentimento, em cumprimento do direito de informação do titular: «os destinatários ou categorias de destinatários dos dados», cfr. art.º 10.º, n.º1, c) da LPDP;

QUALIDADE DOS DADOS

Segundo o Princípio da Qualidade dos dados, os dados pessoais devem ser: tratados de forma lícita e com respeito pelo princípio da boa-fé; recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível; adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados; exatos e atualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou retificados os dados inexatos ou incompletos; conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior., A CNPD pode autorizar a conservação por um período superior, caso haja interesse legítimo, de dados para fins históricos, estatísticos ou científicos, cfr. art.º 5.º (Qualidade dos dados).

HABEAS DATA E DIREITOS ARCO

A Constituição da República Portuguesa assegura de forma expressa ao titular dos dados, entre outras garantias de proteção de privacidade e de dados pessoais, os direitos de acesso, de retificação e de atualização, cuja regulamentação acomete ao legislador ordinário, cfr. art.º 35.º CRP.

O legislador nacional ao transpor a Diretiva n.º 95/46/CE consagrou os «Direitos do titular dos dados» (Secção IIII do Capítulo II), regulamentando em pormenor numa Secção específica da Lei de Proteção de Dados Pessoais, os Direitos de Informação (art.º 10.º), de Acesso (art.º 11.º) e de Oposição (art.º 12.º).

O direito de informação obriga a prestar, nomeadamente, a seguinte informação ao titular no momento da recolha dos dados: identidade do responsável; finalidades do tratamento; os destinatários ou categorias de destinatários dos dados; o carácter obrigatório ou facultativo da resposta e consequências se não responder; a existência e condições do direito de acesso e de retificação, cfr. art.º 10.º da LPDP.

Os direitos de acesso e de retificação significam que o titular tem direito a obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos: a confirmação de serem ou não tratados dados que lhe digam respeito, bem como informação sobre as finalidades desse tratamento, as categorias de dados sobre que incide e os destinatários ou categorias de destinatários a quem são comunicados os dados; a comunicação, sob forma inteligível, dos seus dados sujeitos e quaisquer informações sobre a origem dos dados; o conhecimento da lógica subjacente ao tratamento; a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra a LPDP, nomeadamente, devido ao carácter incompleto ou inexato dos dados; a notificação aos terceiros a quem os

dados tenham sido comunicados de qualquer retificação, apagamento ou bloqueio efetuado, salvo se comprovadamente impossível.

No caso particular dos dados de saúde —incluindo os dados genéticos—, o direito de acesso à informação é exercido por intermédio de médico escolhido pelo titular dos dados, cfr. art.º 1.º, n.º 5 LPDP.

SEGURANÇA

No que diz respeito à segurança do tratamento e confidencialidade, cabe ao responsável pelo tratamento pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente, quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito; estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger.

Conforme tivemos já oportunidade de referir, no caso de tratamento de dados sensíveis (cfr. art.º 7.º LPDP), ao responsável incumbe adotar especiais medidas de segurança para conseguir obter autorização prévia junto da CNPD (cfr. artigos 15.º e 28.º LPDP).

Caso recorra a um subcontratante para o tratamento, o responsável deve escolher um subcontratante que ofereça garantias suficientes em relação às medidas de segurança técnica e de organização do tratamento e deverá zelar pelo cumprimento dessas medidas. As operações de tratamento devem ser regidas por um contrato escrito ou ato jurídico que vincule o subcontratante ao responsável e estipular que o subcontratante apenas atua mediante instruções do responsável e que lhe incumbe igualmente o cumprimento das obrigações que o responsável tem de cumprir, cfr. artigo 14.º LPDP.

O responsável do tratamento e as pessoas que, no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções, cfr. art.º 17.º LPDP.

RESPONSÁVEL PELO PROCESSAMENTO E COMPUTAÇÃO EM NUVEM

Atualmente na legislação portuguesa não existe ainda qualquer referência ou indicação específica a respeito de *Cloud Computing* e proteção de dados pessoais. Sendo no entanto de referir que, ao responsável pelo tratamento incumbe uma obrigação de segurança no tratamento (qualquer operação sobre dados pessoais, cfr. art.º 3.º, b) LPDP), devendo adotar as medidas técnicas e organizativas necessárias, para assegurar —atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação—, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger, cfr. art.º art.º 14.º, n.º 1 LPDP.

AUTORIDAD DE CONTROL. INSCRIPCIÓN O REGISTRO DE TRATAMIENTO

A Constituição da República Portuguesa, contém diversos comandos dirigidos ao legislador ordinário em matéria de proteção de dados pessoais consagrando, nomeadamente, a proteção através de uma entidade administrativa independente, cfr. art.º 35.º, n.º 2 CRP.

Essa entidade administrativa independente é, em Portugal, a Comissão Nacional de Proteção de Dados (CNPD), de âmbito nacional, que possui poderes de autoridade e funciona junto da Assembleia da República, cfr. art.º 21.º LPDP, www.cnpd.pt.

A CNPD, é composta por sete membros, sendo o Presidente e dois vogais eleitos pela Assembleia da República, dois vogais, magistrados designados pelos Conselhos Superiores da Magistratura e do Ministério Público, respetivamente e duas personalidades de reconhecido mérito, com um mandato de cinco anos, cfr. art.º 25.º LPDP.

Possui amplas competências (no setor privado e na Administração Pública), designadamente, de: registo; autorização de tratamento de dados, interconexão e utilização para fins não determinantes da recolha; emissão de Pareceres (por ex. Códigos Conduta); bem como de fiscalização e sanção.

A CNPD disponibiliza no seu site oficial, diversos formulários específicos para vários tipos de tratamento (registo e autorização prévia), que podem ser acedidos através do endereço www.cnpd.pt.

A CNPD elaborou, ainda, diversos documentos de orientação sobre as principais temáticas, atis como: saúde, trabalho, acesso a dados pessoais, informação de crédito, fluxos internacionais, videovigilância, marketing, novas tecnologias, telecomunicações, etc., as quais não são, em si, obrigatórias, mas constituem importantes orientações sobre cada tema de tratamento de dados pessoais.

2.11 REPÚBLICA DOMINICANA

Constitución Política de la República Dominicana

Artículo 44.2: Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.

CONTEXTO NORMATIVO

Hasta el año 2013 en la República Dominicana no existía una legislación específica en cuanto a Protección de Datos de Carácter personal se refiere. Existían, y siguen existiendo sin embargo, varios recursos legales de los que los ciudadanos de este país pueden disponer para ejercer su derecho a la autodeterminación informativa. El derecho a la intimidad, el honor y a la propia imagen, por ejemplo, están consagrados en el Artículo 44 de la Constitución Dominicana de 2010.

En dicha Carta Magna también se incorpora el *Habeas Data,* que nace en el ordenamiento jurídico dominicano como una acción de amparo sobre el derecho de autodeterminación informativa, protegido por la Ley n.º 200-04, General de Libre Acceso a la Información Pública, y pasa ahora a convertirse en una acción autónoma, que da carácter constitucional al derecho de autodeterminación informativa antes mencionado.

Adicionalmente existen legislaciones concretas que se han ido desarrollando para atender necesidades específicas alrededor del derecho a la intimidad, al honor y a la protección de datos de carácter personal como lo son:

— Ley General 200-04 sobre Libre Acceso a la Información Pública y su Reglamento de aplicación, Decreto 130-05.

— Ley n.º 288-05 que regula las Sociedades de Intermediación Crediticia y de Protección al Titular de la Información.

— Ley 42-01. Ley General de Salud y su Reglamento General de Hospitales de la República Dominicana, Decreto n.º 351-99.

— Ley n.º 135-11 de SIDA.

— Ley n.º 183-02 Código de Niños, Niñas y Adolescentes.

— Ley n.º 183-02 Monetaria y Financiera.

— Ley n.º 11-92 Código Tributario.

— La Resolución 055-06 del Instituto Dominicano de Telecomunicaciones (INDOTEL) sobre Protección de Datos de Carácter Personal por los Sujetos Regulados.

Atendiendo a esta situación era ya imprescindible esbozar dentro de un único instrumento jurídico los elementos fundamentales para la protección del derecho a la privacidad y la salvaguarda de los datos personales de los ciudadanos dominicanos. Así se aprueba el 26 de Noviembre de 2013 la Ley n.º 172-13 sobre Protección de Datos de Carácter personal.

Debido a su reciente aprobación, la jurisprudencia alrededor de ésta Ley es prácticamente ausente y se está aún a la espera de que se publique su Reglamento de Aplicación.

En cuento a la labor que nos atañe, procedemos a continuación con el análisis de la situación particular de la República Dominicana dentro del objeto de este estudio.

BIEN JURÍDICO PROTEGIDO: DEFINICIÓN DE DATO DE CARÁCTER PERSONAL

La Ley n.º 172-13, sobre Protección de Datos de Carácter Personal, define en su artículo 6.9 los datos de carácter personal como «Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.».

Además hace una aclaración al distinguir entre datos de carácter personal y datos de carácter personal relacionados con la salud:

«6.10 Datos de carácter personal relacionados con la salud: Cualquier información concerniente a la salud pasada, presente y futura, física o mental, de un individuo»

INFORMACIÓN Y CONSENTIMIENTO. OBLIGACIÓN DE TRANSPARENCIA

En cuanto al derecho de información, la Ley n.º 172-13 establece en su artículo 5.3, sobre el derecho a la información lo siguiente:

3. Derecho de información. Cuando se recaben datos personales que requieran del consentimiento del titular de los datos, para que se les pueda dar el tratamiento de datos o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara, explicando:

— La finalidad para la que serán destinados y quiénes pueden ser sus destinatarios o clase de destinatarios.

— La existencia del archivo, registro, banco de datos o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable.

— La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Así mismo en el artículo 5.4, sobre el consentimiento del afectado y la obligación de transparencia que:

4. Consentimiento del afectado. El tratamiento y la cesión de datos personales es ilícito cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias. El referido consentimiento, prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de los datos descritos en el numeral 3 del presente artículo. Están exentos del requisito de consentimiento al que se refiere el presente artículo todos los organismos de investigación y de inteligencia del Estado encargados de la prevención, persecución y castigo de los crímenes y delitos, previa autorización de autoridad judicial competente. Las entidades de intermediación financiera, los agentes económicos y las demás personas físicas o jurídicas que hayan contratado los servicios de información con las Sociedades de Información Crediticia (SIC), antes de solicitar y obtener un reporte de crédito deberán recabar del titular de los datos el consentimiento expreso y por escrito, indicando en dicho permiso que el titular de los datos autoriza a que pueda ser consultado en las bases de datos de las Sociedades de Información Crediticia (SIC). Será responsabilidad de los usuarios contratantes de los servicios de las Sociedades de Información Crediticia (SIC) recabar y guardar los permisos de los titulares de la información por un período de seis (6) meses, a partir del momento en que dicho permiso fue firmado por el titular de la información. Dentro de este plazo, el titular no alegará la falta de su autorización para la consulta a la Sociedad de Información Crediticia (SIC). Los usuarios o suscriptores deberán guardar absoluta confidencialidad respecto al contenido de los reportes de crédito que les sean proporcionados por las Sociedades de Información Crediticia (SIC). En caso de violación al deber de confidencialidad por parte del usuario o suscriptor, éste será el único responsable por su actuación dolosa, así como por su negligencia e imprudencia.

Dicha Ley establece además excepciones sobre la obligación de consentimiento:

Artículo 27. Excepciones al requerimiento de consentimiento. No será necesario el consentimiento para el tratamiento y la cesión de datos cuando:

a) Se obtengan de fuentes de acceso público.

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

c) Se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás informaciones biográficas.

d) Se deriven de una relación comercial, laboral o contractual, científica o profesional con la persona física, y resulten necesarios para su desarrollo o cumplimiento.

e) Se trate de datos personales que reciban de sus clientes en relación a las operaciones que realicen las entidades de intermediación financiera reguladas por la Ley Monetaria y Financiera y de agentes económicos, de las Sociedades de Información Crediticia (SIC), y de las entidades que desarrollan herramientas de puntajes de crédito para la evaluación

del riesgo de los deudores del sistema financiero y comercial nacional, de acuerdo a las condiciones establecidas en el Artículo 5, numeral 4.

f) Así lo disponga una ley.

g) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias.

h) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve el secreto de la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.

i) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

Vale la pena destacar que, sobre los datos especialmente protegidos, se hace una aclaración específica en cuanto a la obligación de consentimiento, recogida en el Art. 76 de la Ley n.º 172-13 «Sólo con el consentimiento expreso y por escrito del afectado pueden ser objeto de tratamiento los datos de carácter personal que revelen opiniones políticas, convicciones, religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Se exceptúan los archivos de datos personales mantenidos por los partidos políticos, sindicatos, iglesias o comunidades religiosas y asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.»

DATOS ESPECIALMENTE PROTEGIDOS Y OTROS TRATAMIENTOS INVASIVOS

La Ley n.º 172.13 define, en su artículo 6.8 los datos especialmente protegidos como: «Datos de carácter personal que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.» Y ordena, en su art. 75, sobre el carácter de esta información que,

Artículo 75. Datos especialmente protegidos. Ninguna persona física puede ser obligada a proporcionar datos sensibles. La persona física podrá proporcionar datos sensibles, si libre y conscientemente decidiera hacerlo por voluntad propia. Queda prohibida la formación de archivos, bancos de datos o registros que almacenen información que directa o indirectamente revele datos sensibles, siempre y cuando la persona física no haya proporcionado el consentimiento correspondiente de manera libre, consciente y voluntaria. Sin perjuicio de ello, las iglesias, las asociaciones religiosas, clínicas y hospitales, y las organizaciones políticas y sindicales, podrán llevar un registro de sus miembros. Los datos sensibles solo pueden ser recolectados y ser objeto de tratamiento de datos cuando medien razones de interés general autorizadas por la ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Por lo que no impide su tratamiento pero si limita la extensión sobre la cual estos datos pueden ser tratados.

En este sentido, en el Art. 70, sobre Archivos de datos personales comunes que contengan datos de carácter personal establecidos por las entidades aseguradoras, la Ley n.º 172-13 nos dice «No obstante lo dispuesto sobre datos especialmente protegidos, pueden ser objeto de tratamiento los datos de carácter personal que se refieren al origen racial, a la salud y a la vida sexual, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios

sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.»

Y añade en el Art. 78 sobre Datos Relativos a la salud «Los establecimientos sanitarios, públicos o privados, y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando los principios del secreto profesional.»

Adicionalmente en el mismo apartado entran en consideración como datos especialmente protegidos, los datos relativos a las infracciones penales:

Artículo 77. Datos de infracciones penales. Los datos de carácter personal relativos a la comisión de infracciones penales sólo serán incluidos en archivos de datos personales, y sólo serán tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio de conformidad con la ley.

CESIONES DE DATOS

Sobre la cesión de datos, el art. 28 de la Ley n.º 172-13, es muy claro y conciso cuando aclara que: «Los datos personales objeto de tratamiento de datos sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario, con el previo consentimiento de por lo menos uno de los titulares de los datos.»

En este mismo sentido, sobre los ficheros de datos de titularidad pública y de cara a la regulación de la cesión de la información contenida en estos, dicha ley nos dice:

Artículo 39. Comunicación de datos entre instituciones de la administración pública. Los datos de carácter personal recogidos o elaborados por la administración pública para el desempeño de sus atribuciones pueden ser comunicados a otras instituciones de la administración pública. La cesión de datos de carácter personal, objeto de tratamiento, que debe efectuar la administración tributaria en el ejercicio de sus competencias, conforme a lo dispuesto en su normativa reguladora, no requerirá el consentimiento del afectado de conformidad con lo establecido en la presente ley.

Vale la pena destacar que, en este sentido, y a diferencia de lo que se puede ver en la legislación de otros países, la norma Dominicana no hace diferencia entre la Cesión de datos y el Acceso a los datos por cuenta de terceros.

CALIDAD DE LOS DATOS

Sobre la calidad y la proporcionalidad de los datos recogidos para tratamiento, la norma está aún muy limitada y apenas viene a decir lo siguiente:

Artículo 2. Calidad de los datos. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando el principio de calidad, es decir:

a) Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados y pertinentes en relación al ámbito y finalidad para los que se hubieren obtenido.

b) Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

c) Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o, en su caso, completados por el responsable del archivo o base de datos

cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular de los datos establecidos en la presente ley.

d) Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

HABEAS DATA Y DERECHOS ARCO

La acción de *Habeas data,* como hemos visto antes, recogida en el Artículo 70 de la constitución Dominicana, constitucionalizando el derecho a la autodeterminación informativa.

Adicional a lo que aparece recogido en la Constitución Dominicana, la Ley n.º 172-13 establece, en su Artículo 7, sobre la Acción de *Habeas Data* lo siguiente: «Sin perjuicio de los mecanismos establecidos para el ejercicio de los derechos de los interesados, éstos podrán ejercer la acción judicial de *habeas data* de conformidad con la Constitución y las leyes que rigen la materia. La acción judicial de *habeas data* procederá para tomar conocimiento de la existencia de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados que se deriven de una relación comercial, laboral o contractual con una entidad pública o privada; o simplemente, para tomar conocimiento de los datos personales que se presuma que existen almacenados en archivos, registros o bancos de datos públicos o privados. En los casos en que se presuma inexactitud, la desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentre prohibido en la presente ley, para exigir su rectificación, supresión o actualización»

Así mismo, recoge la siguiente normativa sobre la Acción de Habeas Data:

Artículo 18. Legitimación activa. La acción de protección de los datos personales o de *habeas data* será ejercida por el afectado, sus tutores, los sucesores o sus apoderados. Cuando la acción judicial sea ejercida por personas jurídicas deberá ser interpuesta por sus representantes legales o los apoderados que éstas designen a tal efecto.

Artículo 19. Legitimación pasiva. La acción judicial procederá con respecto a los responsables y usuarios de bancos de datos públicos y privados destinados a proveer informes, cuando actúen contrario a las disposiciones establecidas en la presente ley.

Artículo 20. Competencia. Será competente para conocer de esta acción el juez del domicilio del demandado, y para el caso de pluralidad de demandados, en el domicilio de uno de ellos.

Artículo 21. Procedimiento aplicable. La acción de *habeas data* se tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo. El registro o el banco de datos, mientras dure el procedimiento, debe asentar o publicar en los informes que la información cuestionada está sometida a un proceso judicial o de impugnación de *habeas data.*

Artículo 22. Trámite de la demanda de *habeas data.* Sometida la acción, el juez requerirá, mediante resolución motivada, al archivo, registro o banco de datos la remisión de la información concerniente al demandante. Podrá, asimismo, solicitar informes sobre el soporte técnico de datos.

Artículo 23. Contestación del informe. Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no obtemperó al pedido efectuado por el interesado.

Artículo 24. Ampliación de la demanda de *habeas data.* Contestado el informe por parte del demandado, en el término de diez (10) días hábiles, el demandante deberá presentar las

pruebas fehacientes de que su caso se trata de una información incorrecta, errónea o inexacta, y podrá exigir la suspensión, rectificación y actualización de aquellas informaciones que afecten ilegítimamente sus derechos.

Sobre los derechos de Acceso, Rectificación, Cancelación y Oposición a la recogida y tratamiento de Datos Personales, a continuación copiamos los artículos al respecto más relevantes incluidos en la Ley n.º 172-13:

Artículo 8. Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Toda persona tiene derecho a que sean rectificados, actualizados, y, cuando corresponda, suprimidos, los datos personales de los que sea titular y que estén incluidos en un banco de datos. El responsable del banco de datos, después de verificar y comprobar la pertinencia de la reclamación, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin, en el plazo máximo de diez (10) días hábiles de recibido el reclamo del titular de los datos o advertido el error o inexactitud. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más requisitos la acción de protección de los datos personales o de *habeas data* prevista en esta ley. En el supuesto de cesión o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro de cinco (5) días hábiles de efectuado el tratamiento del dato. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación contractual o legal de conservar los datos. Durante el proceso de verificación y rectificación del error o inexactitud de la información de que se trate, el responsable o usuario del banco de datos deberá consignar, al proveer información relativa al demandante, la circunstancia de que se encuentra sometida a revisión o impugnación. La rectificación, actualización o supresión de datos personales inexactos o incompletos que existan en registros públicos o privados se efectuará sin cargo alguno para el interesado.

Artículo 9. Independencia de los derechos de acceso, rectificación, cancelación y oposición. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes. No puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

Artículo 10. Derecho de acceso. Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por esta ley. El tratamiento de los datos e informaciones personales o de sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Solicitarán ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos. El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, le corresponderá a sus sucesores universales. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, en los registros oficiales de las entidades, organismos y empresas públicas, así como sus datos registrados en los archivos de las instituciones y las empresas privadas, o en los bancos de datos privados. El usuario del banco de datos debe proporcionar la información solicitada por el titular de los datos dentro de cinco (5) días hábiles posteriores a haber sido hecha de manera personal dicha solicitud, o vía acto de alguacil. Vencido el plazo sin que se satisfaga el pedido, el titular de los datos podrá incoar una acción judicial ante un juzgado de primera instancia para conocer de la existencia y acceder a los datos que de él consten en registros o bancos de datos públicos o privados, conforme al procedimiento previsto en esta ley. La SIC deberá adoptar todos los mecanismos de seguridad con el propósito de garantizar la protección de la confidencialidad de la información crediticia perteneciente al titular de los datos, y que éste pueda acceder, de forma exclusiva, a su propia información.

Artículo 14. Derechos de rectificación y cancelación. Toda persona tiene derecho a que sean rectificados, actualizados, y, cuando corresponda, suprimidos, los datos personales de los que sea titular y que estén incluidos en un banco de datos.

Artículo 15. Bloqueo de datos. La cancelación da lugar al bloqueo de los datos, conservándose únicamente a disposición de los poderes del Estado para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. En todo caso, la supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

Artículo 26. Excepciones a los derechos de acceso, rectificación, cancelación y oposición. Mediante resolución judicial los responsables o usuarios de bancos de datos oficiales pueden denegar el acceso, rectificación o la supresión en función de la protección de la seguridad nacional, del orden y la seguridad pública, o de la protección de los derechos e intereses de terceros. Estas excepciones no pueden interferir con los derechos a que se hace acreedor cada ciudadano y que consagre la Constitución de la República Dominicana. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de crímenes y delitos por la autoridad competente y la verificación de infracciones administrativas.

MEDIDAS DE SEGURIDAD

Sobre las medidas de seguridad para el tratamiento de datos de carácter personal, la normativa es también limitada y aparece recogida en el art. 5 de la Ley n.º 172-13:

5. Seguridad de los datos. El responsable del archivo de datos personales y en su caso, el encargado del tratamiento, deberán adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida, tratamiento, consulta o acceso no autorizado. En consecuencia:

1. Queda prohibido registrar datos personales en archivos, registros o bancos de datos que no reúnan condiciones técnicas de integridad y seguridad.
2. Los aportantes de datos, las Sociedades de Información Crediticia (SIC) y los usuarios o suscriptores deben adoptar las medidas y controles técnicos necesarios para evitar la alteración, pérdida, tratamiento o acceso no autorizado de los datos sobre historial de crédito que manejen o reposen en la base de datos de las Sociedades de Información Crediticia (SIC).
3. Las Sociedades de Información Crediticia (SIC) deben adoptar medidas apropiadas para proteger sus bases de datos contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informáticos.

ENCARGADOS DE TRATAMIENTO Y *CLOUD COMPUTING*

En cuanto a los deberes y responsabilidades de los encargados del tratamiento de datos personales, la norma está aún pendiente de desarrollarse en este sentido.

Así mismo no se dan detalles sobre cómo aplicar la normativa a los servicios en la nube de internet, conocidos también como *Cloud Computing*.

AUTORIDAD DE CONTROL. INSCRIPCIÓN O REGISTRO DE TRATAMIENTO. PROCEDIMIENTOS. SANCIONES

Respecto al establecimiento de una Autoridad de Control para salvaguardar los derechos establecidos por la Ley n.º 172-13, la legislación Dominicana aún no ha establecido la titularidad del organismo pertinente ni sus deberes y responsabilidades.

Al respecto, la Ley sobre Protección de Datos de Carácter Personal se limita a repetir lo que ya se decía en la Ley 288-05 sobre Sociedades de Intermediación Crediticia (SIC) y de Protección al Titular de la Información actualizando la normativa sobre las Sociedades de Información Crediticia.

De la misma manera, la ley n.º 172-13 repite, sobre las sanciones e infracciones lo recogido en la normativa sobre SIC, añadiendo:

Artículo 84. Sanciones excepcionales. Será sancionado con una multa de diez (10) a cincuenta (50) salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios que haya sufrido la persona por causa de violación a su derecho a la privacidad, conforme a las normas del derecho común, la persona física que:

1. Insertara o hiciera insertar, a sabiendas, datos falsos en un archivo de datos personales, de manera dolosa o de mala fe.
2. Proporcionase, de manera dolosa o de mala fe, información falsa a un tercero, contenida en un archivo de datos personales.
3. Accediere a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, de cualquier forma, a un banco de datos personales.
4. Revelare a otra información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

NORMATIVA ESPECÍFICA

Administración pública

Ley n.º 200-04, sobre libre acceso a la información pública, del 28 de julio del 2004. Sobre derecho de información y de acceso a los Expedientes y actas de carácter administrativo:

Artículo 2. Este derecho de información comprende el derecho de acceder a las informaciones contenidas en actas y expedientes de la administración pública, así como a estar informada periódicamente, cuando lo requiera, de las actividades que desarrollan entidades y personas que cumplen funciones públicas, siempre y cuando este acceso no afecte la seguridad nacional, el orden público, la salud o la moral públicas o el derecho a la privacidad e intimidad de un tercero o el derecho a la reputación de los demás.

También comprende la libertad de buscar, solicitar, recibir y difundir informaciones pertenecientes a la administración del Estado y de formular consultas a las entidades y personas que cumplen funciones públicas, teniendo derecho a obtener copia de los documentos que recopilen información sobre el ejercicio de las actividades de su competencia, con las únicas limitaciones, restricciones y condiciones establecidas en la presente ley.

Párrafo: «Para los efectos de esta ley se entenderá por actas y expedientes a todos aquellos documentos conservados o grabados de manera escrita, óptica, acústica o de cualquier otra forma, que cumplan fines u objetivos de carácter público. No se considerarán actas o expedientes aquellos borradores o proyectos que no constituyen documentos definitivos y que por tanto no forman parte de un procedimiento administrativo».

Sobre limitación al acceso en razón de intereses públicos preponderantes:

Artículo 17 k) Información cuya divulgación pueda dañar o afectar el derecho a la intimidad de las personas o poner en riesgo su vida o su seguridad;

Sobre limitación al acceso en razón de intereses privados preponderantes:

Artículo 18. La solicitud de información hecha por los interesados podrá ser rechazada cuando pueda afectar intereses y derechos privados preponderantes, se entenderá que concurre esta circunstancia en los siguientes casos:

1. Cuando se trate de datos personales cuya publicidad pudiera significar una invasión de la privacidad personal. No obstante, la Administración podría entregar estos datos e informaciones si en la petitoria el solicitante logra demostrar que esta información es de interés público y que coadyuvará a la dilucidación de una investigación en curso en manos de algún otro órgano de la administración pública.
2. (…)
3. Cuando se trate de datos personales, los mismos deben entregarse sólo cuando haya constancia expresa, inequívoca, de que el afectado consiente en la entrega de dichos datos o cuando una ley obliga a su publicación.

SOBRE EL CONSENTIMIENTO DEL AFECTADO

Artículo 19. Cuando el acceso a la información dependa de la autorización o consentimiento de un tercero protegido por derechos de reservas o de autodeterminación informativa en los términos de los Artículos 2 y 17 de esta ley, podrá entregarse la información cuando haya sido dado el consentimiento expreso por parte del afectado. Este consentimiento también podrá ser solicitado al afectado por la administración cuando así lo solicite el peticionario o requeriente. Si en el plazo de quince (15) días o de veinticinco (25) días, en el caso que se haya optado por la prórroga excepcional, no hay demostración frente a la administración requerida de que se haya dado el consentimiento al que se refiere este artículo, se considerará, para todo efecto legal, que dicho consentimiento ha sido denegado.

Banca y seguros

Ley 288-05 que regula las Sociedades de Intermediación Crediticia y de Protección al Titular de la Información. Dicha Ley establece sus principios en el Artículo 4 y entre ellos recoge lo siguiente:

I. Acceso de la Persona Interesada:

Toda persona que demuestre su identidad tiene derecho a saber si se está procesando información sobre su historial crediticio, a conseguir una comunicación inteligible de ella, sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, erróneos, injustificados o inexactos.

II. Exactitud:

Los Aportantes de Datos tienen la obligación de verificar la exactitud y pertinencia de los datos que suministran a los BICs, y estos últimos tienen el deber de cerciorarse de que siguen

siendo los más completos posibles, a fin de evitar los errores por omisión y lograr que se actualicen periódicamente.

III. Finalidad:

La finalidad de esta ley es establecer un marco legal para regular las operaciones de los BICs, estableciendo que ninguno de los datos relativos al historial crediticio de una persona debe ser utilizado o revelado con un propósito incompatible con el que se haya especificado en la presente ley, imponiendo un periodo de conservación de los datos relativos al historial crediticio de una persona que no exceda del necesario para alcanzar la finalidad con que se ha registrado, así como, estableciendo los procedimientos que garanticen de forma ágil y expedita las correcciones reclamadas por los consumidores cuando aparezcan informaciones erróneas o perimidas sobre el historial crediticio de los mismos.

IV. Reserva o Confidencialidad:

Todas las personas físicas o morales, las entidades públicas o privadas, debidamente reconocidas como usuario o suscriptor de un BIC, que tengan acceso a cualquier información relacionada con el historial de un cliente o consumidor, de conformidad con esta ley, deberán guardar la debida reserva sobre dicha información, y en consecuencia, no podrán revelarla a terceras personas, salvo que se trate de autoridad competente. Los funcionarios públicos o privados que con motivo de los cargos que desempeñen tengan acceso a la información de que trata esta ley, están obligados a guardar la debida reserva, aun cuando cesen en sus funciones.

V. Seguridad de Datos:

a) Los Aportantes de Datos, los BICs y los usuarios o suscriptores deben adoptar las medidas y controles técnicos necesarios para evitar la alteración, pérdida, tratamiento o acceso no autorizado de los datos sobre historial de crédito que manejen o reposen en las Bases de Datos de los BICs; y b) Los BICs deben adoptar medidas apropiadas para proteger sus Bases de Datos contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informáticos.

Sobre la modificación, rectificación y cancelación de la información almacenada en las bases de datos de información crediticia (BIC) establece:

Artículo 20. Cuando consumidores no estén conformes con la información contenida en un reporte proveniente de un BIC, podrán presentar una reclamación.

Sobre la proporcionalidad y la calidad de los datos recogidos ordena en su Artículo 29 lo siguiente:

1. La recolección de información no podrá efectuarse por medios fraudulentos o ilícitos.
2. La información recolectada solo podrá ser utilizada para los fines señalados en la presente ley.
3. La información será lícita, actualizada, exacta y veraz, de forma tal que responda a la situación real del titular de la información en un momento determinado. Si la información resulta ser ilícita, inexacta o errónea, en todo o en parte, deberán adoptarse las medidas correctivas, según sea el caso, por parte de los BICs. A efectos de determinar el momento se deberá, en cada reporte, señalar la fecha del reporte.

Derechos fundamentales

La Constitución de la República Dominicana recoge en su Art. 44 el Derecho a la Intimidad y el honor personal, consagrándolo de la siguiente manera:

Artículo 44. Derecho a la intimidad y el honor personal. Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley. Por tanto:

1. El hogar, el domicilio y todo recinto privado de la persona son inviolables, salvo en los casos que sean ordenados, de conformidad con la ley, por autoridad judicial competente o en caso de flagrante delito.
2. Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.
3. Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente, de conformidad con la ley.
4. El manejo, uso o tratamiento de datos e informaciones de carácter oficial que recaben las autoridades encargadas de la prevención, persecución y castigo del crimen, sólo podrán ser tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio, de conformidad con la ley.

SOBRE EL *HABEAS DATA*

Artículo 70. *Habeas data*. Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística.

Por otro lado, la Ley n.º 183-02 que establece el Código de Niños, Niñas y Adolescentes establece los derechos a la intimidad, el honor y la propia imagen para los menores de edad:

Art. 18. Derecho a la intimidad. Todos los niños, niñas y adolescentes tienen derecho al honor, reputación e imagen propia, a la vida privada e intimidad personal y de la vida familiar. Estos derechos no pueden ser objeto de injerencias arbitrarias o ilegales del Estado, personas físicas o morales. (…)

Art. 26. Derecho a la protección de la imagen. Se prohíbe disponer o divulgar, a través de cualquier medio, la imagen y datos de los niños, niñas y adolescentes en forma que puedan afectar su desarrollo físico, moral, psicológico e intelectual, su honor y su reputación, o que constituyan injerencias arbitrarias o ilegales en su vida privada e intimidad familiar o que puedan estigmatizar su conducta o comportamiento.

Párrafo: 3 «La violación de las prohibiciones indicadas en los artículos anteriores se sancionará de la manera dispuesta por el artículo 411 de este Código».

Salud

Ley 42-01. Ley General de Salud.

Art. 28. Todas las personas tienen los siguientes derechos en relación a la salud:

(…)

e) A la confidencialidad de toda la información relacionada con su expediente y con su estancia en instituciones prestadoras de servicios de salud pública o privada. Esta confidencialidad podrá ser obviada en los casos siguientes: cuando sea autorizado por el paciente; en los casos en que el interés colectivo así lo reclame y de forma tal que se garantice la dignidad y demás derechos del paciente; por orden judicial y por disposición de una ley especial;

Reglamento General de Hospitales de la República Dominicana. Decreto n.º 351-99.

Art. 39.1 Son derecho de los pacientes.

c) La Privacidad y confidencialidad durante su atención, protegiendo su integridad social y sicológica.

Art. 35. Se prohíbe terminantemente extraer los expedientes clínicos y las historias clínicas del hospital, a excepción de aquellos casos con previa autorización expresa del Director General. Sólo en caso de requerimiento legal por una autoridad competente, podrán emitirse fotocopias, autentificadas por el jefe de registro y por el Subdirector Médico.

El departamento de registros médicos deberá tener un reglamento que describa las normas nacionales al respecto y describa los procedimientos locales para el manejo de las historias clínicas. Los datos obtenidos en el expediente clínico o la historia clínica son para uso médico científico docente y legal, y todo el personal del hospital está obligado a mantener reserva sobre el contenido del mismo, siendo sancionable la falta de discreción sobre estos aspectos.

Ley n.º 135-11 de SIDA

Artículo 13. Derecho a la confidencialidad. Las personas con el VIH o con SIDA tienen derecho a la confidencialidad en cuanto a su estado de salud, en consecuencia:

1. No están obligadas a informar a su empleador o compañero de trabajo acerca de su condición de salud respecto al VIH/SIDA.
2. Nadie puede comunicar la condición de salud de una persona con VIH o con SIDA, de manera pública o privada, sin su consentimiento previo, salvo las excepciones establecidas en la presente ley.
3. El personal de salud que conozca la condición de salud de una persona con el VIH o con SIDA, debe respetar su derecho a la confidencialidad en lo relativo a los resultados de los diagnósticos, las consultas y la evolución de su condición de salud.

Telecomunicaciones

La Resolución 055-06 del Instituto Dominicano de Telecomunicaciones (INDOTEL) sobre Protección de Datos de Carácter Personal por los Sujetos Regulados.

Art. 4. Información a suministrar en la recogida de Datos directamente de los propios interesados.

4.1 Los Sujetos Regulados que, en sus relaciones con los Interesados, les soliciten Datos de Carácter Personal, deberán informarles de forma previa a su recogida y de modo expreso, preciso e inequívoco de, al menos, los siguientes extremos:

a) De que los Datos de Carácter Personal serán almacenados en un Archivo de Datos de Carácter Personal al objeto de ser Tratados;

b) De las características de dicho Tratamiento;

c) De la finalidad de la recogida de los Datos de Carácter Personal;

d) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean formuladas;

e) De las consecuencias de la obtención de los Datos de Carácter Personal o de la negativa a suministrarlos;

f) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación de acuerdo con lo dispuesto en el Título IX de esta Norma; y

g) De la identidad y dirección del Sujeto Regulado o, en su caso, dirección en la cual el Sujeto Regulado haya fijado domicilio en la República Dominicana de acuerdo con lo dispuesto en la normativa aplicable.

Párrafo: No será necesaria la información a que se refiere la letra (d) del apartado 4.1, si el contenido de ella se deduce claramente de la naturaleza de los Datos de Carácter Personal que se solicitan o de las circunstancias en que se recaban.

Art. 6. Obligación de obtener el consentimiento.

El Tratamiento de los Datos de Carácter Personal por parte de los Sujetos Regulados requerirá del consentimiento previo e inequívoco de los Interesados, salvo cuando la presente Norma prevea expresamente otra cosa.

Art. 43. Derecho de acceso.

43.1 Los Interesados tienen derecho a solicitar y obtener gratuitamente del Sujeto Regulado la siguiente información:

a) Datos de Carácter Personal del Interesado que son sometidos a Tratamiento por el Encargado del Tratamiento;

b) Origen de dichos Datos; y

c) Comunicaciones realizadas o que se prevén hacer de los mismos.

43.2. La información mencionada en el apartado 43.1 podrá obtenerse mediante los siguientes procedimientos a elección del Interesado:

a) La mera consulta de los Datos por medio de su visualización; o

b) La indicación de los Datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

43.3. El Sujeto Regulado tendrá la obligación de hacer efectivo el derecho de acceso del Interesado en el plazo de diez (10) días laborables a contar desde la recepción de la solicitud de acceso del Interesado.

43.4. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a seis (6) meses, salvo que el Interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Art. 44. Derecho de Rectificación y Cancelación.

44.1. Los Interesados tienen derecho a que sean rectificados o cancelados, en su caso, los Datos de Carácter Personal cuyo Tratamiento no se ajuste a lo dispuesto en la presente Norma y, en particular, cuando tales Datos resulten inexactos o incompletos.

44.2. Si los Datos rectificados o cancelados hubieran sido Comunicados previamente, el Sujeto Regulado deberá notificar la rectificación o cancelación efectuada a quien se hayan Comunicado, en el caso de que se mantenga el Tratamiento por este último, que deberá también proceder a la rectificación y cancelación siendo en todo caso el Sujeto.

Regulado responsable ante el INDOTEL y los Interesados en caso de que el cesionario no cancele dichos Datos de Carácter Personal, sin perjuicio de las responsabilidades que el Sujeto Regulado pueda repetir en tal cesionario, en su caso.

44.3. El Sujeto Regulado tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del Interesado en el plazo de quince (15) días laborables a contar desde la recepción de la solicitud de rectificación y/o cancelación del Interesado.

44.4. La cancelación por el Interesado de sus Datos de Carácter Personal no será de aplicación respecto del tratamiento de dichos Datos de Carácter Personal por el Sujeto Regulado a los exclusivos efectos de ejercitar aquellas acciones que en Derecho procediesen frente al Interesado o, en su caso, de defenderse ante las acciones ejercitadas por el Interesado. Dichos Datos de Carácter Personal no podrán ser tratados por el Sujeto Regulado más que con la finalidad aquí señalada, siendo eficaz la cancelación respecto a cualquier tratamiento distinto del aquí expresamente mencionado.

JURISPRUDENCIA RELEVANTE

Sentencia TC/0042/12 del Tribunal Constitucional Dominicano, del 21 de septiembre de 2012

«Los nombres y apellidos de un individuo, aunque constituyen un medio para identificarlo como persona, no son datos que afectan a la esfera más íntima de su titular, ni consideradas informaciones personales sensibles, como sí lo serían, por ejemplo, las cuestiones ideológicas, las características personales, las condiciones de salud, la orientación sexual y el origen.»

«El Tribunal Constitucional considera que, aunque el derecho a la intimidad es un valor fundamental del sistema democrático, al igual que la protección a los datos personales, no pueden, de manera general, aunque sí excepcionalmente, restringir el derecho de libre acceso a la información pública, ya que limitarlo despojaría a la ciudadanía de un mecanismo esencial para el control de la corrupción en la Administración Pública. En ese sentido, el tribunal que dictó la sentencia recurrida acogió la acción de amparo, en razón de que consideró que los datos requeridos por el accionante no eran de carácter confidencial.»

Esta sentencia es de especial interés puesto que establece, dentro del ordenamiento jurídico dominicano, que los nombre y los apellidos de un individuo no se pueden considerar datos personales sensibles.

Sentencia TC/0011/12 del Tribunal Constitucional Dominicano, del 3 de mayo de 2012

«A la luz de la precedente exposición, el Tribunal Constitucional estima que la divulgación no consentida de datos contenidos en los registros de la Dirección General de Migración resulta un ejercicio desproporcionado del derecho a la información, que vulnera el núcleo esencial del derecho fundamental a la dignidad, la integridad, la intimidad y el honor de las personas registradas, cuando carezca de incidencia en asuntos de interés colectivo y concierna personas cuya relevancia pública no haya sido alegada ni tampoco establecida»

En su Sentencia TC/0157/13, el Tribunal Constitucional Dominicano ha considerado, sobre el alcance de la acción de *habeas data* que:

«no es solo para acceder y proteger los datos que se encuentran en bancos de datos o burós de créditos previamente autorizados para su operación por la ley, sino que alcanza también la protección de datos que sobre una persona se encuentren en cualquier registro, público o privado. Es decir, esta protección se extiende a los datos que existan almacenados sobre una persona, independientemente del carácter u origen de los datos o del tipo de registro o banco de datos».

«el derecho de *habeas data* incluye la posibilidad de acceder a los datos que de una persona consten en los registros de su empleador, así como a obtener su corrección.»

«en los registros laborales de las instituciones y empresas se encuentra una cantidad importante de informaciones personales de sus empleados, relativas al desarrollo de su relación laboral, como pueden ser promociones, aumentos de salario, reconocimientos, amonestaciones, suspensiones e incluso la terminación de esa relación laboral, sus razones y su forma, es decir, desahucio, despido, entre otras; y los errores o imprecisiones que puedan constar en su historial laboral pudiendo afectarles otros derechos consagrados en la Constitución.»

Sobre la información recogida en fichas policiales que se almacenen en registros públicos, la Sentencia TC/0027/13 del Tribunal Constitucional dictamina:

«[e]l mantenimiento de dicha ficha, por parte de la Policía Nacional, luego de haberse establecido que el referido ciudadano no ha tenido expediente penal a cargo, constituye una grave violación a los derechos invocados por él, lo que deviene un obstáculo para que alcance de manera plena su libre desarrollo personal y pueda convivir dignamente en la sociedad.»

«ninguna (…) persona, aun tratándose de un condenado a penas privativas de libertad, puede ser mantenido soportando de por vida el fardo de antecedentes penales destacados en registros de acceso público, lo que constituye un serio obstáculo para el ejercicio de importantes prerrogativas ciudadanas, en especial el derecho a no ser discriminado pudiendo, en determinados casos, generar daños irreparables.»

2.12 URUGUAY

Constitución de la República Oriental de Uruguay

Artículo 7: Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad (…).

El 11 de agosto de 2008 en Uruguay se promulgo la Ley de Protección de Datos, introduciendo nuevos elementos jurídicos tanto a bases de datos públicas como a privadas.

La ley en ese país viene a reconocer a la protección de datos como derecho fundamental, comprendiendo la información de cualquier tipo, registrada en cualquier soporte que la haga susceptible de tratamiento. Ha definido que el responsable de la Base de Datos puede ser una persona privada o pública, estatal o no estatal, donde el titular de los datos puede ser una persona determinada o determinable, física o jurídica, a esta última se extiende la protección en cuanto corresponda[122].

Uruguay ha sido considerado un país adecuado a la normativa europea, ha adherido al Convenio n.º 108 para la protección de las personas con respecto al tratamiento automatizado

---

[122] Felipe Rotondo, Disponible en: http://www.redipd.org/actividades/encuentros/VII/common/felipe_rotondo_ppt_uruguay.pdf, 2/09/2014.

de datos de carácter personal, y se encuentra participando activamente en las instancias relativas a su modificación.

BIEN JURÍDICO PROTEGIDO

El legislador Uruguayo ha indicado en la Ley «… establecer un marco jurídico claro y necesario para garantizar y hacer efectivo uno de los derechos fundamentales del ser humano, como es el derecho a la protección de los datos de carácter personal y por tanto de la intimidad de las personas.» Tal como se expresa en los propios informativos del Gobierno Uruguayo[123], el derecho a la protección de datos personales es un derecho humano amparado en la Constitución y en la Ley n.º 18.331. La Ley reconoce el derecho a controlar el uso que se hace de los datos personales. Ésta se aplica a los datos personales registrados en cualquier soporte que permite tratarlos y usarlos posteriormente de diversos modos, tanto en el ámbito privado como público.

El Objeto de la Normativa uruguaya claramente se centra en las experiencias y necesidades internacionales (así como también las exigencias), centrándose en el *Habeas Data,* es decir el control que a cada uno de los ciudadanos uruguayos les corresponde sobre la información que concierne personalmente, sea íntima o no, para preservar, en último término, el libre desarrollo de su personalidad, individualidad y privacidad en lo referido a la denominada «Autodeterminación Informativa»[124].

INFORMACIÓN Y CONSENTIMIENTO. OBLIGACIÓN DE TRANSPARENCIA

El sistema uruguayo de protección de datos personales tiene un alto grado de formalidad, especialmente en las peculiaridades que exige al consentimiento como la legitimación para un tratamiento conforme lo ha querido el legislador.

La Ley que comunica normas de carácter general sobre la protección de datos personales en Uruguay, prevé que para el tratamiento de cada dato personal contenido en una base de datos debe recabarse el consentimiento del titular de dicho dato personal.

El no cumplimiento de dicho requisito hace que la base de datos sea literalmente ilegal. La norma es clara en señalar que es prioritario informar al titular en forma expresa, precisa e inequívoca por medios claros, sencillos y gratuitos acerca de: la finalidad para la cual será tratado el dato, quiénes pueden ser los destinatarios del dato, la existencia de una base de datos, la identidad y domicilio de su responsable, la actividad desarrollada por el responsable de las bases de datos, el carácter obligatorio o facultativo de las respuestas al cuestionario (especialmente cuando se trata de datos sensibles), las consecuencias de proporcionar datos, las consecuencias de la negativa a proporcionar datos, las consecuencias de proporcionar datos inexactos, la posibilidad de ejercer el derecho de acceso, rectificación y supresión.

Los autores[125] señalan que cumplida esta instancia inicial de información, el titular del dato debe manifestar su consentimiento, con el objeto de que su dato sea recopilado de acuerdo con la ley, cuya expresión debe ser: libre, inequívoca, informada, previa a la utilización del dato y expresa.

Esto particularmente interesante debido a que permite «ceder» cierto grado de responsabilidad en la persona y su derecho a saber sobre quién tiene sus datos, dónde los tiene, para qué los tiene y que va a hacer con ellos, lo que supone un acto de transparencia informativa

---

123 http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_bp_ur_g_1.pdf, 4/09/2014.

124 La lectura de diversas fuentes permite identificar un alto compromiso con la norma internacional y los derechos humanos, con un fuerte componente de la LOPD Española. Nota del Autor.

125 http://www.rlpdp.com/2012/09/ana-brian-nougreres-consentimiento/, 7/092014.

donde el responsable de la base de datos debe recabar y guardar la prueba de la existencia del consentimiento o de la negativa a darlo, por parte del titular, a través de cualquier medio conforme a derecho.

Es claro si que las excepciones al principio datos sensibles, los datos referentes a telecomunicaciones, datos cuya finalidad es la publicidad, datos referentes a actividades comerciales o crediticios, además de los contenidos en bases de datos creadas y/o reguladas por leyes especiales, términos y definiciones que encontramos en las diversas legislaciones respecto a datos personales.

DATOS ESPECIALMENTE PROTEGIDOS Y OTROS TRATAMIENTOS INVASIVOS

De acuerdo a la propia información de Gobierno Uruguayo, la Ley identifica además datos que por sus características deben ser especialmente protegidos[126].

a) Los datos sensibles: Son aquellos que revelan un origen racial o étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referidas a la vida sexual de una persona.

b) Los datos relativos a la salud: Se trata de informaciones o de datos concernientes a la salud física o mental de una persona. Por ejemplo, el porcentaje de discapacidad y su información genética. Se trata de los datos que son tratados en los establecimientos sanitarios, públicos o privados y por los profesionales de la salud quienes, guardando el deber del secreto profesional, manejan datos personales relativos a la salud de los pacientes, de acuerdo con la legislación sanitaria y de la protección de datos. Los datos también podrán ser tratados cuando sea necesario para salvaguardar la vida del afectado o de otra persona.

c) Los datos relativos a las telecomunicaciones: Las personas físicas o jurídicas, públicas o privadas, que actúen en el mercado de las telecomunicaciones, en cualquiera de sus segmentos, como titulares o responsables de un servicio, deberán garantizar la protección de los datos personales cumpliendo con las exigencias legales.

d) Los datos relativos a bases de datos con fines publicitarios: Consisten en datos que se tratan con el propósito de establecer perfiles determinados con fines promocionales, comerciales o publicitarios, o que permiten establecer hábitos de consumo, cuando esos datos figuren en documentos accesibles al público, hayan sido facilitados por sus titulares u obtenidos con su consentimiento.

e) Los datos relativos a la actividad comercial o crediticia: Está autorizado el tratamiento de datos destinados a informar sobre la solvencia patrimonial o crediticia, cuando los mismos sean obtenidos de fuentes de acceso público o procedan de informaciones facilitadas por el acreedor o en las circunstancias previstas en la Ley. Para el caso de las personas jurídicas (empresas u organizaciones) también se permite el tratamiento de toda información autorizada por la normativa vigente.

CESIONES DE DATOS

La transcripción del articulado de la Ley Uruguaya expresa claramente la idea representativa de las cesiones de datos, es así como en su Artículo 14.º Sobre los Derechos referentes a la comunicación o la cesión de datos, se expresa lo siguiente:

---

126 http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_bp_ur_g_1.pdf, 8/09/2014.

«La comunicación o la cesión de datos a terceros, solamente procede para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y destinatario de ésta, previo consentimiento del titular de los datos a quien se le debe informar inequívocamente la finalidad de dicha comunicación, identificando al destinatario y el tipo de actividad que desarrolla.

No se considera comunicación o cesión de datos el acceso por parte de un encargado de tratamiento, que resulte necesario para la prestación de un servicio al responsable, salvo que este acceso implique la existencia de un nuevo vínculo entre el encargado del tratamiento y el titular».

CALIDAD DE LOS DATOS

La legislación uruguaya enfrento este principio desde una perspectiva superior, lo que a juicio propio, otorga un mayor valor al concepto de calidad incorporando en su Artículo 5.º, dentro de sus principios generales, el siguiente valor:

«Valor y fuerza. La actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales: Legalidad, Veracidad, Finalidad, Previo consentimiento informado, Seguridad de los datos, Reserva y Responsabilidad.

Esto amplía el espectro de la definición habitual en las legislaciones sobre esta materia, incorporando valores superiores al espectro de la calidad, lo que incluye totalidad, exactitud, autorización y mantención de dichos datos cuando correspondiera. Llama la atención la claridad respecto a la conjugación con las normas ISO/IEC 27000[127].

HABEAS DATA Y DERECHOS ARCO

La Ley 18.331 Uruguaya, ajustándose a la legislación europea, incorpora también la tercera línea de protección de datos, la acción del *Habeas Data,* en su Artículo 37. El que señala: «toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y —en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización— a exigir su rectificación, inclusión, supresión o lo que entienda corresponder. Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso.»

MECANISMOS DE CONTROL

La Legislación Uruguaya crea la Unidad Reguladora y de Control de Datos Personales[128], como Organismo de Control. De acuerdo a la información que publican, las facultades de esta unidad, respecto a la Ley son:

— Asistir y asesorar a las personas.

— Dictar normas y reglamentaciones.

— Realizar un censo de las bases de datos incluidas en la ley de protección de datos. Mantener registro de los censos.

---

127 http://www.agesic.gub.uy/innovaportal/file/509/1/Directrices_para_la_aplicacion_de_la_Ley_N_18.331_V2.0.pdf.

128 http://www.datospersonales.gub.uy/.

— Controlar el cumplimiento de las normas sobre integridad, veracidad y seguridad. Solicitar información sobre el tratamiento de los datos.
— Emitir opinión respecto a sanciones administrativas por el incumplimiento de la ley. Asesorar al Poder Ejecutivo en proyectos de ley que refieran a la protección de datos personales.
— Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables.

OTRAS NORMAS RELACIONADAS

La creación de un órgano de control sobre la materia en Uruguay tiene vital importancia para el desarrollo del derecho a la protección de datos personales. Esto sin duda ha permitido la implementación de diversas actividades dirigidas a sensibilizar y educar a la población en el conocimiento y la importancia de la protección de sus datos, así como en el fortalecimiento del ejercicio de los derechos, permitiendo con esto empoderar en la normativa. Esto ha permitido que otras normas como la de bancos, la Tributaria, Salud, entre otras, tengan un centro común en materia de datos personales, siendo esta última la que permite otras garantías que establece la ley y que resultan de gran relevancia son las asociadas a las potestades de la Unidad respecto a los responsables de bases de datos, entre ellas, las relativas a la posibilidad de solicitar información y a la realización de controles sobre los mecanismos que circunscriben a los datos personales en la realidad actual de los países más avanzados en estas materias.

3. PAÍSES CON LEGISLACIÓN EN MATERIA DE PRIVACIDAD

3.1 PARAGUAY

Constitución de la República del Paraguay

Artículo 135: Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

TRATAMIENTO DEL *HABEAS DATA* EN LA CONSTITUCIÓN PARAGUAYA

El derecho a la intimidad se encuentra recogido en el artículo 33 de la Constitución de la República del Paraguay: «la intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas».

El artículo 135 de la Carta Magna reconoce que «toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos», elevando al concepto de garantía constitucional el *habeas data*.

En la configuración del sistema constitucional paraguayo, la garantía del *habeas data* se define en dos fases: en primer lugar la capacidad de acceder a los registros donde obran datos del afectado con la finalidad de verificar los mismos. En un segundo término se contempla la capacidad de modificar, actualizar o cancelar los datos que obran en los mismos, cuando los datos fuesen erróneos o afecten a determinados derechos personalísimos del afectado.

Este procedimiento, ordinario, se rige por el Código de Procedimientos Civiles, y se encuentra exento de tasas judiciales. Cabe recordar que el artículo 136 de la Constitución paraguaya establece que «ningún magistrado judicial que tenga competencia en podrá negarse a entender en las acciones o recursos previstos en los artículos anteriores; si lo hiciese injustificadamente, será enjuiciado y, en su caso, removido. En las decisiones que dicte, el magistrado judicial deberá pronunciarse también sobre las responsabilidades en que hubieran incurrido las autoridades por obra del proceder ilegítimo y, de mediar circunstancias que *prima facie* evidencien la perpetración de delitos, ordenará la detención o suspensión de los responsables, así como toda medida cautelar que sea procedente para la mayor efectividad de dichas responsabilidades. Asimismo, si tuviese competencia, instruirá sumario pertinente y dará intervención al magistrado competente para su persecución.»

NORMATIVA SOBRE LA INFORMACIÓN DE CARÁCTER PRIVADO

La Ley n.º 1682, modificada por la Ley n.º 1969, el 2 de setiembre de 2002, que reglamenta la información de carácter privado tiene por objeto «regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares», quedando exentas las bases de datos o fuentes de informaciones periodísticas o las libertades de emitir opinión y de informar.

En su artículo 2 la norma reconoce que «toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado», haciendo referencia en el artículo 3 que «es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas», es decir la información se trate de forma disociada y no se permita la identificación de las personas, prohibiéndose la publicidad o difusión de datos de carácter personal de las personas.

El concepto de datos sensibles se desarrolla en la citada norma, haciendo referencia a los referentes a pertenecías raciales o étnicas, preferencias políticas estado individual de salud, convicciones religiosas filosóficas o morales, intimidad sexual, así como aquellos otros que fomenten prejuicios y discriminaciones, o afecten a la dignidad, privacidad, intimidad e imagen personal y familiar.

En relación al tratamiento y publicidad de los datos económicos, solvencia o cumplimiento de obligaciones comerciales y financieras, se establece un número *clausus* haciendo referencia a que las personas hubiesen otorgado autorización expresa y por escrito para que obtengan sobre las obligaciones no reclamadas judicialmente; cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar en cumplimiento de disposiciones legales; o cuando consten en fuentes públicas de información.

Sobre la publicación y difusión se recogen tres supuestos: los datos consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil ocupación o profesión, lugar de trabajo y teléfono ocupacional; cuando se trate de datos solicitados por el propio afectado; o cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto.

Dichos datos serán actualizados permanentemente por las empresas, personas o entidades que los almacenen, procesen y difundan, en relación a la situación patrimonial, solvencia económica y cumplimiento de las obligaciones derivadas.

Las empresas y entidades deberán comunicar en el plazo de dos días la actualización del crédito atrasado que ha generado la inclusión del deudor. En este sentido la Ley establece que la actualización, modificación o eliminación de los datos será absolutamente gratuita, debiendo proporcionarse además, a solicitud del afectado y sin costo alguno, copia auténtica del registro alterado en la parte pertinente.

El acceso a los datos podrá realzarse por el afectado sobre sus propio datos, los de su cónyuge o sobre las personas que acredite se hallen bajo su tutela o curatela, o sobre bienes, que se encuentren detallados en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial, así como

conocer el uso que se haga de los mismos o su finalidad, tal y como recoge el artículo 8 de la citada Ley.

La norma establece un sistema de sanciones en su artículo 10:

— Las personas físicas o jurídicas que publiquen o distribuyan información sobre la situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales y financieras en violación de las disposición de esta Ley serán sancionadas con multas que oscilan, de acuerdo con las circunstancias del caso, entre cincuenta y cien jornales mínimos para actividades laborales diversas no especificadas, multas que se duplicarán, triplicarán, cuadruplicarán, y así sucesivamente por cada reincidencia del mismo afectado.

  Para que se produzca la multa, la duplicación, triplicación, cuadruplicación, etc., se requerirá que la entidad reacia al cumplimiento de la actualización dentro del plazo establecido en el Artículo 7.º de esta Ley, haya recibido el previo reclamo por escrito del particular afectado;

— Las personas físicas o jurídicas que, pese a estar obligadas a rectificar o a suministrar información para que se rectifiquen datos de acuerdo con lo que dispone el Artículo 7.º, no lo hagan o lo hagan fuera de los plazos allí establecidos, serán sancionadas con multas que, de acuerdo con las circunstancias del caso, oscilarán entre cincuenta y cien jornales mínimos para actividades laborales diversas no especificadas; multas que, en caso de reincidencia, serán aumentadas de acuerdo con la pauta establecida en el apartado a).

  Para que se produzca la multa, duplicación, triplicación, cuadruplicación, etc., se requerirá que la entidad reacia al cumplimiento de la actualización dentro del plazo establecido en el Artículo 7.º de esta Ley, haya recibido el previo reclamo por escrito del particular afectado;

— Si los reclamos extrajudiciales a los que se refiere el Artículo 8.º no fueran atendidos sin razón o sin base legal, se aplicará a la entidad reacia al cumplimiento de sus obligaciones, una multa que, de acuerdo con las circunstancias del caso, oscilará entre cien y doscientos jornales mínimos para actividades laborales diversas no especificadas.

OTRA NORMATIVA APLICABLE

El Código Penal paraguayo recoge diferentes tipos delictivos relacionados con la protección de la intimidad, la privacidad, el derecho al honor y la propia imagen de las personas, sírvase a título enumerativo y no limitativo, los siguientes:

Artículo 143. Lesión de la intimidad de la persona.

1. El que, ante una multitud o mediante publicación en los términos del artículo 14, inciso 3.º, expusiera la intimidad de otro, entendiéndose como tal la esfera personal íntima de su vida y especialmente su vida familiar o sexual o su estado de salud, será castigado con pena de multa.
2. Cuando por su forma o contenido, la declaración no exceda los límites de una crítica racional, ella quedará exenta de pena.
3. Cuando la declaración, sopesando los intereses involucrados y el deber de comprobación que según las circunstancias incumba al autor, sea un medio adecuado para la persecución de legítimos intereses públicos o privados, ella quedará exenta de pena.

4. La prueba de la verdad de la declaración será admitida sólo cuando de ella dependiera la aplicación de los incisos 2.º y 3.º.
5. La persecución penal dependerá de la instancia de la víctima.

Artículo 146 b. Acceso indebido a datos.

1. El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa.
2. Como datos en sentido del inciso 1.º, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible.

Artículo 146 c. Interceptación de datos.

El que, sin autorización y utilizando medios técnicos:

1. obtuviere para sí o para un tercero, datos en sentido del Artículo 146 b, inciso 2.º, no destinados para él;
2. diera a otro una transferencia no pública de datos; o
3. transfiriera la radiación electromagnética de un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor.

Artículo 148. Revelación de secretos privados por funcionarios o personas con obligación especial.

1. El que revelara un secreto ajeno llegado a su conocimiento en su actuación como:

— funcionario conforme al artículo 14, inciso 1.º, numeral 14; o
— perito formalmente designado,

será castigado con pena privativa de libertad de hasta tres años o con multa.

2. La persecución penal del hecho dependerá de la instancia de la victima. Se aplicará lo dispuesto en el artículo 144, inciso 5.º, última parte.

En el ámbito del tratamiento e implantación de la firma electrónica en Paraguay cabe citar la Ley n.º 4017, de 23 de diciembre de 2010, de validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico y el Decreto n.º 7369, de 23 de septiembre de 2011, por el que se aprueba el Reglamento de la Ley n.º 4017/10.

También encontramos normativa relacionada con el ámbito de la protección de datos en el establecimiento y regulación del comercio electrónico mediante la Ley n.º 4868, de 26 de febrero de 2013 y el Decreto n.º 1165, de 27 de enero de 2014, por el que se aprueba el Reglamento de la Ley n.º 4868, de Comercio Electrónico. Así como la regulación del marco de aplicación de las tecnologías de la información y comunicación en el sector público y creación de la Secretaría Nacional de Tecnologías de la Información y Comunicación por la Ley n.º 4989, de 9 de agosto de 2013.

3.2 PUERTO RICO

Constitución del Estado Libre Asociado de Puerto Rico

Sección 8: Toda persona tiene derecho a protección de ley contra ataques abusivos a su honra, a su reputación y a su vida privada o familiar.

BIEN JURÍDICO PROTEGIDO

La Constitución del Estado Libre Asociado de Puerto Rico, dentro de la sección 8, reconoce de manera somera los derechos a la privacidad, honra y vida privada y en la sección 10 reconoce la protección a los registros y no intercepción de comunicaciones privadas.

A pesar de que dentro de la sección 19, se comunica de manera expresa que aquellas garantías que no fueron enunciadas dentro de la carta de derechos no suponen su exclusión para con la sociedad, uno se debe cuestionar porque la falta de anunciamiento respecto al derecho a la propia imagen, cuya protección normalmente se prevé a nivel constitucional en la mayoría de los Estados. Es por ello, como mencionaré en el desenlace de la jurisprudencia, que la imagen debe recibir una protección constitucional, es la única forma de garantizar una tutela apropiada.

No se reconoce la acción de *habeas data* dentro su constitución por lo que como anteriormente se decía, se deja cierto vacío o puerta cerrada ante futuras acciones para garantizar la autodeterminación informática, de igual manera, el hecho de que no se conciba este tipo de tutelas a nivel constitucional, refleja el interés del estado para precautelar esta esfera de sus ciudadanos.

JURISPRUDENCIA

Colón *vs.* Romero Barceló (D.P.R. 573)

No existe jurisprudencia que enuncie, reconozca de forma clara el *habeas data* o brinde mayor protección y doctrina vinculante en cuanto a los datos personales, sin embargo, la presente sentencia constitucional, reconoce y protege a nivel constitucional el derecho a la propia imagen y a su vez el derecho a la intimidad.

Mediante la presente sentencia se reguló el tratamiento sin autorización de la información respecto a ciudadanos fallecidos, tomando en cuanto que estos actos constituyen una violación a la intimidad de los familiares.

En los hechos se había utilizado la imagen del difunto para una publicidad televisiva de tinte político, por lo que se vieron vulnerados los derechos de los interesados que en este caso vendrían a ser los herederos del difunto.

Esta sentencia pone el derecho a la propia imagen por encima del derecho a la primera a la expresión en su vertiente política.

NORMATIVA RELACIONADA A LA PROTECCIÓN DE DATOS

Ley n.º. 139 de 13 de julio de 2011 de protección a la propia imagen. Producto de la jurisprudencia anteriormente mencionada, se dicta la Ley de protección a la propia imagen, en la cual se reconocen quienes son los sujetos con legitimidad para tratar con la imagen de uno mismo o de terceros, se reconoce la figura de sátira y parodia, lo cual indica un cierto avance en cuanto al derecho de la propia imagen.

La imagen es parte de un dato personal, por lo que se logró subsanar un gran vacío normativo que mantenía este Estado en cuanto a la tutela de este tipo de datos personales.

Ley n.º 39 de 24 de enero de 2012 de Notificación de Política de Privacidad. Esta ley significa un gran avance en materia de protección de datos personales, tomando en cuenta los antecedentes legislativos de Puerto Rico, una normativa como esta sinónimo de un cambio

radical en el tratamiento de datos, inclusive se podría considerar como la primera y más efectiva a nivel legislativo.

En el art. 2 reconoce la obligación a todo aquel sujeto que recopile datos de enunciar de manera clara que tipo de información está siendo recolectada, indicar cuál es el procedimiento para revisar dicha información.

Falta a una normativa como esta, enunciar los principios básicos de la protección de datos, por lo menos el de finalidad, y es algo que se pudo haber incluido tranquilamente en un inciso del art. 2.

4. PAÍSES CON LEGISLACIÓN EN MATERIA DE *HABEAS DATA*

4.1 BOLIVIA

Constitución Política del Estado

Artículo 21: Las bolivianas y los bolivianos tienen los siguientes derechos: 2. a la privacidad, intimidad, honra, propia imagen y dignidad.

EL *HABEAS DATA* EN LA CONSTITUCIÓN POLÍTICA DEL ESTADO

La Constitución política del Estado de Bolivia reconoce dentro de sus derechos civiles en su artículo 21 el derecho a la intimidad, la honra, la privacidad y la propia imagen, es normal ver este tipo de derechos aglomerados dentro de un mismo título, y esto se debe a que cuando uno es afectado de manera consecuente se vulnera el otro, esa es la razón por la cual el derecho a la propia imagen se protege junto a la privacidad, intimidad y honra, sin embargo hasta la fecha, dentro de Bolivia no se ha desarrollado una doctrina clara sobre la diferencia entre la privacidad e intimidad, es más se maneja ambos conceptos como uno solo, y eso a posterior podría generar conflictos de índole jurídico, esto se explicara en lo concerniente a la acción de *habeas data*. A pesar de la falta de distinción conceptual, en cuanto a la tutela, siempre será positivo para un Estado, el tener dentro de su constitución el reconocimiento de estos bienes jurídicos.

EL *HABEAS DATA,* ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

La Constitución política del Estado reconoce la autodeterminación informática, y esto es posible de manera judicial a través de la acción de protección de privacidad, anteriormente llamada *habeas data*. A criterio del presente autor, el nombre de «acción de protección a la privacidad» no devela el verdadero alcance y naturaleza de esta acción, puesto que la privacidad no es lo único que se protege cuando uno ejerce su autodeterminación informática, pero aun así el nombre que adopto esta acción desde la última reforma constitucional.

En Bolivia el uso de esta acción no se ha comprendido a totalidad, por lo cual se limita a proteger los daños a la imagen y reputación, cuando en si los alcances y efectos podrían ser aún mayores, tomando en cuenta que existen pocas pero ya emergentes instituciones que comercian con datos e información de personas cuya voluntad y conocimiento no ha sido prestada para esta comercialización.

Posiblemente falta cultura de protección de datos y por ello no se ha podido utilizar esta acción de la manera correcta, en el entendido de que hasta la fecha no se entiende que se debe proteger, y es porque los datos personales aún no se conciben como un bien jurídico tutelado, al menos no para el saber del ciudadano de a pie, sino que se lo ve como algo accesorio a la privacidad o intimidad, sin hacer distinción de estas dos últimas palabras.

JURISPRUDENCIA BOLIVIANA

Sentencia constitucional 0965/2004-R del Recurso de *habeas data* de fecha 23 de junio de 2004

Esta acción es interpuesta antes de la modificación constitucional, por lo cual aun conserva el nombre de *habeas data*. Se interpone el recurso de *habeas data* interpuesto por José Carrasco Vidaurre contra Gerardo Tórrez Ossio, Gerente General del periódico «La Razón» y Efraín Óscar Alarcón Bautista.

El señor Efraín Óscar Alarcón Bautista, realiza una publicación en el periódico La Razón, indicando que el accionante es un deudor moroso, hecho que según el accionante vulnera su derecho a la honra, dignidad, privacidad.

Los recurridos por su parte demuestran y acreditan que el accionante realmente es deudor moroso, entre otras cosas indican que la acción de *habeas data* debe proteger información sensible, como un hecho de violación, pero el exigir el cumplimiento de una deuda no vulnera los derechos fundamentales.

El gerente de el periódico La Razón, se manifiesta y entre lo más importante de su informe, se rescata el conocimiento a la naturaleza subsidiaria de la acción de *habeas data,* recalcando que el accionante nunca le solicito de manera prejudicial el conocimiento o rectificación de la información, y posiblemente lo más importante que manifiesta el recurrente es cuando indica que «…no es un banco de datos, es un instrumento por el que se exteriorizan ideas,…»[1]

El fallo de la Corte, declara improcedente la acción al igual que la sala anterior que conoció el proceso, dentro de los fundamentos jurídicos del fallo constitucional, es importante ampliar que la Corte mediante doctrina, desarrollo la acción de *habeas data,* describiendo su alcance en cuanto al conocimiento, rectificación, anulación, actualización de datos, indica de igual manera que el periódico La Razón no es ni tiene una base de datos, sino que es un instrumento de información mediante el cual como servicio, puede poner al conocimiento de sus lectores, publicaciones a pedido, sin embargo, a pesar de no ser satisfecha la petición del accionante, este puede ejercer su derecho a réplica solicitar por medio de la institución que se publique otra nota para desvirtuar lo mencionado sobre el accionante.

Sentencia Constitucional 1972/2011-R Sucre, 7 de diciembre de 2011

Esta sentencia fue interpuesta después de la modificación constitucional, por lo que hace referencia a la acción de protección a la privacidad. Rosalía Angulo Barrios contra Rubén Suárez Camiña, Jefe Departamental de la Fuerza de Lucha Contra el Narcotráfico (FELCN) de Santa Cruz.

El accionante había solicitado que se eliminen antecedentes penales que existían registrados en la base de datos de la Fuerza de lucha contra el narcotráfico, esto porque nunca se le había proseguido un proceso contra su persona, sin embargo el accionado indicó que la solicitud debía ser por orden judicial.

El accionado indicó que por no haber eliminado aquellos datos erróneos al momento de su petición, se estaba incurriendo contra su derecho al trabajo y dignidad, por lo cual solicita que

---

[1] Sentencia Constitucional 0965/2004-R del Recurso de *habeas data* de fecha 23 de junio de 2004, disponible en red: http://www.redipd.org/documentacion/jurisprudencia/common/bolivia/SENTENCIA_CONSTITUCIONAL_0965.pdf.

se declare probada la acción y se ordene la eliminación de datos en la base de datos de la FELCN. La otra parte, indica que no se le está negando la eliminación de datos, es más se le indica al accionante cual es el procedimiento para realizarlo.

En el fallo se deniega la tutela, y esto a causa del principio de subsidiariedad el cual es importante tomar en cuenta antes de solicitar esta acción, tomando en cuenta que existían mecanismos para eliminar la información y no se usaron las vías pertinentes, es por ello sustancialmente que el juez negó la petición.

LEYES RELACIONADAS A LA PROTECCIÓN DE DATOS

Código Penal. Modificado por la Ley n.º 1768, de 10 de marzo de 1997. Mediante el Código Penal se intentó tutelar los datos informáticos, específicamente en su art. 363 ter se penaliza su acceso, modificación y eliminación no autorizada.

La corriente penal, nunca debe ser la única vía u opción estatal para proteger un bien, los delitos informáticos en Bolivia, son muy amplios y vacíos, sumados con la falta de comprensión respecto a los datos e información uno llega a nada, no es más que un tipo penal cuya medida legislativa no es más que eso, una orden descrita en un código pero dificultosa para asegurar mediante las pocas herramientas con las que cuenta el Estado y la ignorancia sobre la materia en cuanto a los administradores de justicia.

Y es una ignorancia plural, no se ha inculcado mediante doctrina que es el dato personal y su importancia para con el ciudadano, es por ello que una medida penal no marca la diferencia.

Decreto Supremo n.º 1793, de 13 de noviembre de 2013. Este Decreto Supremo, a nivel legislativo, es el más completo en cuanto a la protección de datos personales, esto porque de manera tácita señala los principios que salvaguardan la información de las personas.

— Habla sobre el Consentimiento, cuya exigencia es nueva dentro de la normativa boliviana, y gestora de una adecuada autodeterminación informática.

— Notificación y finalidad. Esto sigue el principio de propósito específico, es decir, que desde que los datos serán recolectados uno debe ser comunicado con el propósito que se trataran sus datos.

Otra avance legislativo dentro de este Decreto Supremo, es la obligación que impone al que trata los datos, para identificarse y explicar su domicilio y como poder ser ubicado.

Si bien esta ley es un gran avance dentro de la protección de datos, es necesario mencionar algunos aspectos que podrían haber mejorado, como el hecho de que la protección de datos, es solo un artículo con 4 incisos dentro del presente Decreto Supremo, el mismo que de manera global regula todo lo concerniente a las tecnologías de comunicación e información, lo cual hace que englobe muchos aspectos y no logre brindar el desarrollo pertinente, siendo consecuente con la crítica, es necesario señalar, que se debería haber explicado la importancia de los datos personales íntimos y la tutela correspondiente cuando estos sean tratados, dejando mecanismos rápidos, accesibles y eficaces, para su anulación en la base de datos, más efectivo hubiera sido, la prohibición de este tipo de datos.

Es importante de igual manera recalcar, que un Estado puede avanzar de manera legislativa, pero si es que de manera conceptual no se ha logrado entender la importancia de la protección de datos, entonces las normas no serán más que letra muerta aplicándose en ocasiones remotas.

4.2 BRASIL

Constitución de la República Federativa del Brasil

Artículo 5: LXXII se concederá «*habeas data*»: a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo (…) LXXVII son gratuitas las acciones de «*habeas corpus*» y «*habeas data*» y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía.

O *Habeas Data* é instrumento constitucional de proteção de direitos individuais relativamente recente no Brasil, haja vista sua previsão ter aparecido pela primeira vez por meio da Constituição da República de 1.988. Seus traços recentes ainda se devem ao fato de sua regulamentação ter acontecido apenas no ano de 1.997 (Lei Ordinária n.º 9.507), quase dez anos após sua previsão constitucional.

Sua origem guarda relação com outros dois remédios constitucionais, o *Habeas Corpus* e o Mandado de Segurança. Quanto ao primeiro sua relação é bem restrita ao fato de ambos se referirem à ações constitucionais que visam a proteção de direitos individuais. Já no que diz respeito ao segundo, o Mandado de Segurança, sua relação é mais estreita. Antes da Constituição de 1.988 era o Mandado de Segurança o instrumento a ser utilizado por aqueles que pretendiam ter acesso a informações pessoais, sendo este considerado um direito líquido e certo que justificava a utilização do mandamus. Outro fator que os aproxima é que, mesmo após a Constituição, a ação de *Habeas Data* por não possuir regulamentação própria era regida pelas normas referentes ao Mandado de Segurança, sendo que tal situação perdurou durante 9 anos até a aprovação da lei que regulamentou a ação de *Habeas Data*.

Atualmente o *Habeas Data* no Brasil está previsto no art. 5.º, inciso LXII, da CRFB de 1.988, e é regulamentado pela Lei Ordinária n.º 9.507 de 12 de novembro de 1.997.

A Constituição Federal assim prevê a ação de *habeas data*:

Artigo 5: Inciso LXXII – Conceder-se-á *habeas data*:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.[2]

O *Habeas Data*, conforme previsto na Constituição brasileira, servirá para aquelas situações em que o indivíduo pretenda ter acesso às informações ao seu respeito seja para que possa conhece-los ou até mesmo promover alguma correção. Nas palavras do insigne Alexandre de Morais.

Assim, pode-se definir o *habeas data* como o direito que assiste a todas as pessoas de solicitar judicialmente a exibição dos registros públicos ou privados, nos quais estejam incluídos seus dados pessoais, para que deles se tome conhecimento e se necessário for, sejam retificados os dados inexatos ou obsoletos ou que impliquem em discriminação.[3]

---

[2] BRASIL. Constituição da República Federativa do Brasil. 1.988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 14 de setembro de 2014.

[3] MORAES, A.: *Direito constitucional*. São Paulo: Atlas, 2013. p. 154.

A previsão do direito de acesso e retificação de dados pessoais implica, mesmo que indiretamente, na proteção destes mesmos dados pessoais, que apesar de não ter sido expressa no texto constitucional é possível extraí-la tanto desta previsão da ação de h*abeas data,* como da previsão de proteção à vida privada e intimidade, constantes do inciso X, do art. 5.º, da Constituição Federal. O que eleva o objeto desta ação à categoria de direitos e garantias fundamentais.

Contudo o direito de acesso e retificação de informações estão adstritos aos bancos de dados de «entidades governamentais ou de caráter público», como previsto na Constituição. A Lei n.º 9.507/97, no parágrafo único do art. 1.º (o caput fora vetado), assim define os bancos de dados acessíveis por esta ação: «Considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações»[4].

A interpretação literal do estabelecido pela Constituição levaria à restrição do espectro de alcance da presente ação, totalmente inadequado à realidade, visto que não apenas os entes governamentais formam bases de dados com caráter público, mas especialmente a iniciativa privada. Não obstante a previsão deste remédio constitucional tenha sido motivada pelas constantes repressões vividas pelos brasileiros no período anterior à Constituição em razão do longo período de Ditadura Militar.

A melhor interpretação é justamente aquela que leva em consideração o caráter público não de quem elaborou os registros, mas sim dos próprios registros naqueles casos em que podem ser acessados ou transmitidos a terceiros. Sendo tal entendimento reforçado pelo próprio Código de Proteção e Defesa do Consumidor brasileiro (Lei n.º 8.078/90).

Tal interpretação pode ser observada na ementa de caso julgado pelo Tribunal de Justiça do Estado de Minas Gerais:

Habeas data-Órgãos de proteção ao crédito-caráter público-legitimidade passiva-informação incompleta-interesse processual. 1. Os órgãos de proteção ao crédito, tais como SPC e SERASA, são considerados de caráter público, nos termos do parágrafo único do art. 1.º da Lei 9.507, de 12 de novembro de 1997, devendo submeter-se às disposições atinentes ao *habeas data,* no tocante aos registros e informações cadastrais mantidos em seus bancos de dados. 2. Negada, pela entidade de proteção ao crédito, a informação solicitada, ou sendo esta prestada de maneira incompleta, legítimo é o interesse da pessoa em servir-se do *habeas data* para obtê-la. (TJMG-Apelação Cível 1.0702.06.283404-0/001, Relator(a): Des.(a) Guilherme Luciano Baeta Nunes, 18.ª CÂMARA CÍVEL, julgamento em 16/10/2007, publicação da súmula em 31/10/2007) (grifo nosso).[5]

ASPECTOS PROCESSUAIS

A Lei n.º 9.507/97 cuidou de regulamentar especialmente os aspectos processuais que devem ser observados pelos interessados em impetrar a ação de *habeas data.* Para tanto estabeleceu requisitos que extrapolam aqueles derivados da própria petição inicial exigidos pela norma processual vigente (Código de Processo Civil, arts. 282 a 285).

---

4 BRASIL. Lei n.º 9.507 de 12 de novembro de 1.997. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9507.htm Acesso em: 15 de setembro de 2014.

5 BRASIL. Tribunal de Justiça de Minas Gerais. Apelação Cível 1.0702.06.283404-0/001, Relator(a): Des. (a) Guilherme Luciano Baeta Nunes, 18.ª CÂMARA CÍVEL, julgamento em 16/10/2007, publicação da súmula em 31/10/2007. Disponível em: http://www5.tjmg.jus.br/jurisprudencia/formEspelhoAcordao.do Acesso em 10 de setembro de 2014.

Afim de que o impetrante possa se utilizar do *habeas data* é imprescindível que o mesmo faça primeiro um requerimento administrativo ao ente responsável pela base de dados e somente após sua negativa é que, juntando a prova da negativa, poderá impetrar a competente ação de *habeas data*. Tal exigência, apesar de vista com muita reserva, é o entendimento firmado pelo Supremo Tribunal Federal por meio da Súmula n.º 02-Não cabe o *habeas data* (CF, art. 5..º, LXXII, a) se não houve recusa de informações por parte da autoridade administrativa».

Sobre o posicionamento supra citado Alexandre de Morais entende que não obstante a posição do Supremo Tribunal Federal e do Superior Tribunal de Justiça tal interpretação é contrária à própria Constituição Federal, visto que em momento o constituindo fez tal exigência.

Entendemos por esses motivos que o parágrafo único do art. 8..º da Lei n..º 9.507/97 deve ser interpretado conforme a Constituição Federal, no sentido de não se exigir em todas as hipóteses a prova de recusa do órgão competente ao acesso às informações ou da recusa em fazer-se a retificação, ou ainda, da recusa em fazer-se a anotação, mas tão-só nas hipóteses em que o impetrante, primeiramente, optou peio acesso às instâncias administrativas.[6]

A exigência de negativa em processo administrativo anterior faz com que o instrumento que seria utilizado para proteção de dados se torne ineficaz em razão da falta de interesse do próprio cidadão conforme relata o próprio Superior Tribunal de Justiça em matéria veiculada no sítio do órgão no dia 02 de setembro de 2012, onde informa que nos 4 anos anteriores à matéria apenas 54 *habeas data* foram impetrados, tendo apenas um sido concedido.[7]

Para Doneda: «Um sistema de proteção de dados pessoais que tenha como instrumentos principais de atuação o recurso a uma ação judicial (e isso somente após um inafastável périplo administrativo) não se nos apresenta como um sistema adequado às exigências da matéria»[8].

Ainda acerca de aspectos processuais referentes à ação de *habeas data* é importante informar que trata-se de ação personalíssima não sendo admitido o acesso a informações privadas por terceiros, mesmo em se tratando de titular de informações que tenha falecido e o impetrante seja seu sucessor.

A legitimidade ativa da presente ação é estendida também às pessoas jurídicas, visto que as mesmas também são dotadas de personalidade jurídica e o Código Civil brasileiro concedeu à elas a proteção aos direitos da personalidade, como o são os dados pessoais (art. 52). Vale mencionar julgado do Supremo Tribunal Federal acerca de *habeas data* concedido à pessoa jurídica que pretendia ter acesso a banco de dados mantido pela Receita Federal brasileira, gerando inclusive a repercussão geral:

Direito constitucional e administrativo. *Habeas data*. Acesso a informações. Sistema sincor de cadastro. Manifestação pela repercussão geral. Cabimento de *habeas data* para fins de acesso a informações incluídas em banco de dados denominado SINCOR-Sistema de Conta-Corrente de Pessoa Jurídica, da Receita Federal. (RE 673707 RG, Relator(a): Min. LUIZ FUX, julgado em 06/09/2012, ACÓRDÃO ELETRÔNICO DJe-184 DIVULG 18-09-2012 PUBLIC 19-09-2012).[9]

---

6 MORAIS, A.: op. cit. p. 156.

7 BRASIL. Superior Tribunal de Justiça. Coordenadoria de Editoria e Imprensa. *Habeas data:* instrumento raro na defesa do cidadão contra abusos totalitários. Brasília, 02/09/2012. Disponível em: http://stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=106825 Acesso em 20 de setembro de 2014.

8 DONEDA, D.: *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006. p. 337.

9 BRASIL. Supremo Tribunal Federal. RE 673707 RG, Relator(a): Min. LUIZ FUX, julgado em 06/09/2012, ACÓRDÃO ELETRÔNICO DJe-184 DIVULG 18-09-2012 PUBLIC 19-09-2012. Disponível em: http://www.stf.jus.br/portal/jurisprudencia/pesquisarJurisprudencia.asp Acesso em 30 de agosto de 2014.

Quanto à legitimidade passiva a mesma está vinculada ao caráter público ou não da base de dados à qual o impetrante quer ter acesso. Contudo o Supremo Tribunal Federal já expressou entendimento que tal caráter deveria recair também sobre a pessoa do impetrado:

Ementa: *Habeas Data*. Ilegitimidade passiva do Banco do Brasil S.A para a revelação, a ex-empregada, do conteúdo da ficha de pessoal, por não se tratar, no caso, de registro de caráter público, nem atuar o impetrado na condição de entidade Governamental (Constituição, art. 5.º, LXXII, a e art. 173, § 1.º, texto original). (RE 165304, Relator(a): Min. Octavio Galloti, Tribunal Pleno, julgado em 19/10/2000, DJ 15-12-2000 PP-00105 Ement Vol-02016-04 PP-00782 RTJ VOL-00176-01 PP-00396)[10].

No caso acima percebe-se a interpretação restritiva do dispositivo constitucional à qual fizemos menção anteriormente e que prejudica a utilização do *habeas data* no Brasil.

Um último ponto relacionado ao aspecto processual do *habeas data* é a questão da competência para análise do pedido. A mesma será definida em razão da pessoa do Impetrado, variando entre o Supremo Tribunal Federal e os Tribunais de Justiça estaduais, de acordo com o que estabelece a própria Constituição da República.

O *HABEAS DATA* NAS RELAÇÕES DE CONSUMO

A interpretação extensiva da expressão «caráter público» contida na Constituição Federal, bem como na lei que regulamenta a ação de *habeas data,* encontra suporte legal na Lei n.º 8.078 de 1990 – Código de Proteção e Defesa do Consumidor –, mais precisamente no art. 43, § 4.º:

Art. 43... § 4.º-Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.[11]

A mencionada interpretação extensiva, como dito anteriormente, é necessária para que a ação em discussão não restrinja aos bancos de dados administrativos por entes públicos, ou concessionários ou permissionárias, como defende Celso Ribeiro Bastos:

As entidades governamentais compreendem a administração direta e a indireta (autarquias, fundações instituídas pelo Poder Público, sociedade de economia mista e empresas públicas). As entidades de caráter público são as instituições e pessoas físicas ou jurídicas de direito privado prestadoras de serviço público ou de interesse público, na qualidade de concessionárias ou permissionárias. (grifo nosso)

O dispositivo contido no Código de Proteção e Defesa do Consumidor brasileiro resolve a controvérsia ao menos nos casos em que estejam envolvidos direitos do consumidor, já que sendo considerados de caráter público atende diretamente o previsto no parágrafo único do artigo 1.º da Lei n.º 9.507/97.

O que na verdade acaba por atingir a grande maioria dos bancos de dados desenvolvidos atualmente, especialmente aqueles formados por aplicações de internet onde informações das mais diversas possíveis são coletadas indiscriminadamente dando origem aos «big datas».

---

10 BRASIL. Supremo Tribunal Federal. RE 165304, Relator(a): Min. OCTAVIO GALLOTTI, Tribunal Pleno, julgado em 19/10/2000, DJ 15-12-2000 PP-00105 EMENT VOL-02016-04 PP-00782 RTJ VOL-00176-01 PP-00396. Disponível em: http://www.stf.jus.br/portal/jurisprudencia/pesquisarJurisprudencia.asp Acesso em 30 de agosto de 2014.

11 BRASIL. Lei n.º 8.078 de 11 de setembro de 1.990. Código de Proteção e Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm Acesso em 07 de setembro de 2014.

NOTAS SOBRE O MARCO CIVIL DA INTERNET E O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS

O Brasil recentemente aprovou uma lei que regula a utilização da internet dentro do seu território, bem como, está às vistas de aprovação uma legislação destinada exclusivamente à proteção de dados pessoais. Trata-se do Marco Civil da Internet (Lei n.º 12.965 de 23 de abril de 2014), e do Anteprojeto de Lei de Proteção de Dados Pessoais que está sendo desenvolvido pelo Ministério da Justiça brasileiro com previsão de apresentação ao Congresso Nacional no ano de 2014 ou início de 2015.

O Marco Civil da Internet, já em vigor, trata de forma tímida a questão da proteção de dados pessoais, o que não representa um ponto fraco, visto que o mesmo fora elaborado para atuar em conjunto com a futura Lei de Proteção de Dados Pessoais, pela mesma equipe do Ministério da Justiça.

O art. 3.º desta Lei estabelece como um dos princípios da utilização da Internet no Brasil a proteção de dados pessoais, na forma da lei. Fazendo referência direta ao Anteprojeto retro mencionado. Contudo, como esta lei ainda não existe, a proteção será dada conforme os instrumentos que ora já se encontram regulados, como a ação de *habeas data* de que trata o presente artigo.

O Marco Civil no seu artigo 7.º, que regula os direitos e garantias dos usuários de internet no Brasil, em seus incisos VII a X assim estabelece a proteção dos dados pessoais:

Art. 7.º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

VII. não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII. informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

— justifiquem sua coleta;

— não sejam vedadas pela legislação; e

— estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX. consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X. exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;...[12]

Como se depreende da leitura dos dispositivos mencionados a proteção de dados pessoais pelo Marco Civil já representam um avanço específico nesta seara ainda não regulamentada no Brasil.

O Anteprojeto de Proteção de Dados pessoais por sua vez trará princípios, as regras que o setor público e o setor privado deverão cumprir, a existência de uma autoridade pública para regulamentar e administrar a aplicação da lei, seguindo o modelo de outros países como a Itália, por exemplo, bem como preverá sanções civis a serem aplicadas aos que violarem a proteção dos dados pessoais.

---

[12] BRASIL. Lei n.º 12.965 de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em 22 de setembro de 2014.

CONCLUSÃO

Como pode se observar o status de proteção dos dados pessoais no Brasil ainda engatinha, um pouco distante daquele patamar que poderia ser considerado ideal.

A ação de *habeas data* que deveria ser o instrumento hábil à concretização deste objetivo acaba por encontrar uma série de limitações imposta por sua Lei regulamentadora que acabam por afastar a utilização da mesma. Sendo, inclusive, em muitos casos substituída por outro remédio constitucional, o Mando de Segurança.

Acredita-se que com a recente aprovação do Marco Civil da Internet e com a futura aprovação da Lei de Proteção de Dados pessoais, possa o país contar com aparato jurídico adequado à proteção deste que é um direito elevado à categoria de direitos fundamentais constitucionalmente protegidos.

4.3 ECUADOR

Constitución Política de la República del Ecuador

Artículo 66.19: El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

CONCEPTOS RECOGIDOS EN LA CONSTITUCIÓN ECUATORIANA

La Constitución de la República del Ecuador vigente, recoge en diferentes artículos el derecho a la privacidad, la intimidad, el honor y la protección de datos, el artículo 66.19 reconoce «el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley».

La acción del *habeas data* se introduce en el artículo 92, «toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados».

Al tratar la movilidad humana, el artículo 40.5 de la Constitución establece que se «mantendrá la confidencialidad de los datos de carácter personal que se encuentren en los archivos de las instituciones del Ecuador en el exterior».

LA GARANTÍA CONSTITUCIONAL DEL *HABEAS DATA*

El precepto recogido en el artículo 92 de la Constitución, es entendido por la Sala Primera del Tribunal Constitucional de Ecuador, en Sentencia dictada en Quito el 15 de octubre de 2008, como «una garantía constitucional creada para salvaguardar el derecho a la autodeterminación informativa, esto es, mantener el control de los datos que existan sobre una persona o sobre sus bienes, y para proteger el derecho a la honra, a la buena reputación y a la intimidad personal y familiar», entendiendo que la acción es «creada para salvaguardar el derecho a la autodeterminación informativa, procura mantener el control de los datos que existan sobre una persona o sobre sus bienes, y para proteger el derecho a la honra, a la buena reputación y a la intimidad personal y familiar».

El Pleno del Tribunal ecuatoriano recoge que «el derecho a la protección de datos implica, a su vez, el derecho a conocer la existencia de ficheros o de información almacenada y el propósito o la finalidad que se persigue con ellos; el derecho a acceder, que permite a los afectados averiguar el contenido de la información registrada, o participar de la información que sobre la imagen o concepto de ellos se tenga; y el derecho a rectificar, que es la posibilidad del titular afectado de que los datos sobre su persona al ser incorrectos, inexactos y obsoletos sean rectificados en la medida en que, al ser ajenos a la realidad le pueden causar perjuicio».

El *habeas data* en tres derechos implica diferentes derechos de las personas y su garantía correspondiente: acceso, conocimiento, actualización, rectificación, eliminación o anulación de datos. Con la implantación de la citada garantía constitucional se pretende evitar el uso incorrecto de la información, la no actualización y adecuación a la realidad de los datos o la utilización de los mismos para fines diferentes de aquellos para los que fue recopilada, así como la conservación de los datos más allá del periodo para el que fueron recopilados, evitando así, lesiones al honor, el buen nombre o la privacidad de la persona.

Del artículo 92 de la Carta Magna ecuatoriana, se desprenden las diferentes vertientes del *habeas data:* el derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o privadas, con independencia de la forma de tratamiento de dichos datos, teniendo derecho a conocer sobre el uso, finalidad, origen y destino de sus datos; el derecho a la actualización de sus datos, su rectificación, eliminación o anulación.

En este sentido la acción del *habeas data,* nace como instrumento ejercitable por las personas para salvaguardar el derecho a su honor, su privacidad y a que la información que de ellos se tiene sea exacta, pertinente, actualizada, fidedigna y no sea utilizada con otra finalidad.

En el procedimiento debe acreditarse en el proceso la fundamentación, legitimación y carga de la prueba que los sustente, demostrando el daño ocasionado a su honor, buena reputación, a su intimidad, acreditando el daño moral irrogado, así como lo perjuicios causados, en base a la posterior solicitud, ante las jurisdicción civil ordinaria, de la correspondiente indemnización por el afectado.

NORMATIVA RELACIONADA EN MATERIA DE PROTECCIÓN DE DATOS

Entre las diferentes normas ecuatorianas que tratan la protección de datos, cabe citar la Ley n.º 2002-67, de comercio electrónico, firmas electrónicas y mensajes de datos, recoge en su artículo 9 que «para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la

República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato».

En relación a la confidencialidad de la información, el artículo 5 afirma que «se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia».

En sus disposiciones la Ley define que «el derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados», datos personales como «aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley» y datos personales autorizados como «aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular».

La Ley Orgánica de Transparencia y Acceso a la Información, de 18 de mayo de 2004, garantiza el derecho a acceder a las fuentes de información, como mecanismo de participación democrática y de información, su espíritu es recogido en iniciativas como Voto Transparente, desarrollada por el Consejo Nacional Electoral ecuatoriano, donde además de ahondar en los principios democráticos electorales y la rendición de cuentas, procura información sobre protección de datos y privacidad, en aras a una mayor cultura entre los ciudadanos y la protección de sus datos.

La citada Ley Orgánica en su artículo 5 establece que «se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas».

La Ley de burós de información crediticia, recoge en su Título II el manejo de la información crediticia, estableciendo, entre otros conceptos que «sólo con el conocimiento pleno y la autorización previa del titular de la información crediticia, en cada operación, los burós de crédito podrán obtener y mantener en sus archivos la nueva información crediticia distinta de aquella proveniente de la Central de Riesgos. En este caso, los clientes de los burós pondrán en conocimiento de los titulares de la información crediticia, lo siguiente:

a) La existencia de las bases de datos que administran los burós, su finalidad y los potenciales destinatarios de la información;

b) La identidad y dirección de los burós que recepten la información;

c) Las posibles consecuencias del uso de la información;

d) Los derechos que les asisten.»

El artículo 9 de la Ley establece que «el titular de la información crediticia tendrá derecho a:

a) Conocer si en la base de datos de un buró existe información sobre sí mismo y acceder a el a sin restricción alguna; y,

b) Exigir de la fuente de información crediticia, la rectificación de la información ilegal, inexacta o errónea y comunicarla al buró para que éste, de ser el caso, la rectifique.»

La Ley Orgánica de Control Constitucional establece en su artículo 35 que «el *habeas data* tendrá por objeto a) Obtener del poseedor de la información que éste la proporcione al recurrente, en forma completa, clara y verídica; b) Obtener el acceso directo a la información; c) Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y, d) Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado, o no la ha divulgado».

El artículo 36 recoge que «no es aplicable el *habeas data* cuando afecte al sigilo profesional; o cuando pueda obstruir la acción de la justicia; o cuando los documentos que se soliciten tengan el carácter de reservados por razones de Seguridad Nacional. No podrá solicitarse la eliminación de datos o informaciones cuando por disposición de la 68 Ley deben mantenerse en archivo o registros públicos o privados».

La Ley del Sistema Nacional de Registro de Datos Públicos, publicada en el Suplemento número 162 de 31 de marzo de 2010 del Registro Oficial, crea y regula el sistema de registro de datos públicos y su acceso, en entidades públicas o privadas, garantizando la seguridad organización y sistematización de la información, así como la interoperabilidad de la misma, con criterios de eficacia, eficiencia y transparencia.

El Capítulo II de la Ley establece que «las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos son responsable de la integridad, protección y control de los registros y bases de datos a su cargo», se garantiza así mismo la confidencialidad de los datos de carácter personal «ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, condición migratoria y los demás atenientes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales».

El acceso a la información patrimonial de las personas, deberá estar justificado y motivado en la petición, indicando el uso que se le dará a la misma, incurriendo en caso de incumplimiento de dicha finalidad, en responsabilidades. La Administración y su personal deberá adoptar las medidas de seguridad encaminadas a la protección de la información, garantizando su confidencialidad e integridad.

La Ley establece la posibilidad de actualización, rectificación y cancelación o supresión de los datos, así como la aplicabilidad de la garantía constitucional del *habeas data,* en su artículo 21, «el titular de los datos podrá exigir las modificaciones en registros o bases de datos cuando dichas modificaciones no violen una disposición legal, una orden judicial o administrativa. La rectificación o supresión no procederá cuando pudiese causar perjuicios a derechos de terceras o terceros, en cuyo caso será necesaria la correspondiente resolución administrativa o sentencia judicial».

Otras normas reseñables son la Ley Orgánica 2000-21 de Defensoría del Consumidor, la Ley No. 184 especial de telecomunicaciones (Registro Oficial No. 996 10 de agosto de 1992), o en el ámbito sanitario el Código de ética Médica (Acuerdo Ministerial 14660-A. Registro Oficial 5 de 17 de agosto de 1992) que recoge en su Capítulo IX el secreto profesional,

entendido como «un deber que nace de la esencia misma de la profesión. El interés público, la seguridad de los enfermos, la honra de las familias, la responsabilidad del profesional y la dignidad de la ciencia médica, exigen el secreto. Los médicos tienen el deber de conservar en secreto todo cuanto observen, escuchen o descubran en el ejercicio de su profesión».

4.4 GUATEMALA

Constitución Política

Artículo 24: Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.

EL *HABEAS DATA* EN LA CONSTITUCIÓN POLÍTICA DEL ESTADO

Dentro de su Constitución política del Estado, garantiza en 2 artículos la protección a la información que genera cada persona dentro del ámbito de la comunicación. La inviolabilidad se reconoce mediante el su Artículo 24 donde indica: «Inviolabilidad de correspondencia, documentos y libros. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna».[13]

La importancia de la información reside en su capacidad de identificarlo y hacerlo identificable, y es el titular quien decide cual es el destino final de estos datos, se debe entender que en medio de todos los datos que conforman la información existen ciertos aspectos de la vida que si bien pueden ser mencionados o confiados a determinada persona o entidad, el contenido de esta información no pretende llegar a un público masivo y desconocido, puesto que estos «también describen aspectos más sensibles o delicados sobre el individuo, como son los datos personales sensibles que tiene que ver con la forma de pensar, estado de salud, características físicas, ideología o vida sexual, entre otros.»[14]

Posiblemente el mayor problema del artículo 24 anteriormente citado, sea que a nivel constitucional, solo se protege la información que pueda ser vulnerada en un ámbito de comunicación, y no así se garantiza una protección a los datos que sean recopilados por bases de datos privadas, que utilicen esta información con fines comerciales.

Dentro del Artículo 31 de la Constitución política del Estado de Guatemala se reconoce el *Habeas Data,* sin embargo, y es necesario recalcarlo, se refiere a archivos y registros estatales, y solo sobre estos datos recae la autodeterminación informática del titular, lo cual es algo incompleto para la extensión que usualmente reviste al *habeas data* en otros países.

JURISPRUDENCIA GUATEMALTECA

Corte de constitucionalidad de Guatemala, expediente 1356-2006

En la jurisprudencia emitida, se puede observar el caso del Procurador de los Derechos Humanos (patrocinando a F.R.A.A.) *vs*. Informes en Red, Sociedad Anónima. El amparo es

---

13 Constitución Política del Estado República de Guatemala.

14 Texto extraído de investigación sobre ley de acceso a la información pública y protección de datos, co autores, Licda. Rosa María Juárez, Licda. Iris Hernández.M.Sc. Mario Sánchez, Disponible en línea: http://www.redipd.org/actividades/talleres/La_Antigua_02_2014/common/Ponencias_Taller_La_Antigua./GUATEMALA.pdf última vez revisado 08/09/2014.

motivado a causa de que: el accionado vende información privada de ciudadanos, entre ellos el accionante F.R.A.A, esta información que es publicada sin permiso del titular, ha generado daños a su prestigio y en consecuencia a esto, conllevó conflictos para conseguir trabajo.

Se han vulnerado los derechos a la dignidad, el honor, la privacidad y la intimidad de una persona, y a la protección de los datos personales que figuran en programas informáticos. Finalmente la corte falla a favor de F.R.A.A, preservando su autodeterminación informática.

LEGISLACIÓN RELACIONADA A LA PROTECCIÓN DE DATOS

Ley de Acceso a la Información Pública de Guatemala. Decreto 57-2008. Esta normativa se encarga de coadyuvar a la transparencia, y garantizar al ciudadano de a pie, poder verificar la información que almacenan todas las entidades estatales, esta ley cumple con el fin propio de su naturaleza, pero es necesario diferencia la finalidad de cada normativa o por lo menos comprender su prioridad en cuanto al espíritu de la norma, mencionando que la presente ley busca en si la transparencia de las actividades relacionadas a la información por parte del Estado, no así la protección de datos.

De igual manera los ciudadanos tienen la autodeterminación informática sobre estas bases de datos estatales, para conocer, modificar, eliminar la información. Esto no a causa de la presente ley, sino del artículo 24 de la constitución política del Estado.

Ley de Derecho de Autor y Derechos Conexos. Decreto 33-1998. Cuando se habla de protección de datos, no se puede excluir la ley de derechos de autor y derechos conexos, puesto que en esta normativa se protegen los programas de ordenador y las bases de datos, por lo que no deja de ser pertinente al tema referido de protección de datos.

Sin embargo el término datos, para esta ley, no se la observa con el sentido amplio que normalmente se maneja, en cuanto a información referida a una persona, sino que se entra en la génesis del derecho informático, y se habla del conjunto de bits que forman un programa o software.

Son los programas de ordenador, la producción sujeta a derechos de autor más violentada por parte de los ciudadanos, es normal ver copias ilegales en países en vías de desarrollo, y todo esto es parte del comercio informal, la presente ley pretende enmarcar el ilícito de la reproducción indebidamente promovida.

Ley de Protección al Consumidor y Usuario. Decreto 006-2003. En lo relacionado a la protección de datos, no existe mayor novedad dentro de esta normativa, salvo la conminación hacia los funcionarios de la entidad encargada de recibir las quejas por parte de los consumidores, se pretende asegurar la protección de los datos de aquel consumidor que realice un reclamo, esto siempre y cuando la queja haya sido manifestada por un medio electrónico.

Ley para el reconocimiento de las Comunicaciones y Firmas Electrónicas. Decreto 47-2008. En cuanto a la firma electrónica la regulación que se da respecto a los datos, va en sentido de la validez de los datos, bajo el principio de no repudio, poniendo en igualdad a los datos obtenidos por un medio electrónico a los obtenidos por un medio tradicional como ser el papel.

Cuando hablamos de comercio electrónico, firma electrónica y comunicaciones, se debe entender la información desde otro ángulo, uno en el que los datos e información de los contratantes por ley deben ser visibles y disponibles para su ulterior consulta, con la aclaración de que solo las partes contratantes y el tercero de confianza pueden acceder a esta información.

Código Penal. Decreto 17-1973. En cuanto al aparato punitivo del Estado, se puede observar que avanzo bastante en cuanto a los delitos informáticos, castigando a aquellas personas que

destruya o inutilice registros informáticos, de igual manera existe una pena para aquel que modifique los programas informáticos.

Un avance muy interesante que sale de este Código Penal, es el art. 274 D que castiga a quien crea una base de datos o registro con intenciones de dañar la intimidad de la persona mediante la recolección de datos íntimos. Un delito muy peculiar dándole el protagonismo de sujeto activo a quienes creen la base, esto tiene alcances internacionales en el caso de que la base sea transfronterizo por el *cloud computing*.

Cuando se promueven delitos informáticos en este caso para proteger los datos privados, se debe tener en cuenta, que las políticas criminales deben ser integrales, tanto en la norma sustantiva como en la adjetiva, es decir, de nada sirve un tipo penal, si de manera procedimental y yendo más lejos, de manera fáctica no existen los mecanismos apropiados para no solo demandar sino realizar los actos investigativos de manera adecuada.

4.5 HONDURAS

Constitución de la República de Honduras

Artículo 76: Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen.

EL *HABEAS DATA* EN LA CONSTITUCIÓN POLÍTICA DEL ESTADO

La Constitución del Estado Centroamericano de Honduras de 1982, en su artículo 76 reconoce el derecho al honor, a la intimidad personal, familiar y a la propia imagen de las personas. Este precepto se completa con lo estipulado en el artículo 182 donde «el Estado reconoce la garantía de *Habeas Corpus* o Exhibición Personal, y de *Habeas Data*», concretamente, prosigue la Carta Magna hondureña, en relación al *habeas data,* que «toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en caso de que fuere necesario, actualizarla, rectificarla y-o enmendarla. Las acciones de *Habeas Corpus* y *Habeas Data* se ejercerán sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o, días hábiles o inhábiles y libre de costas. Únicamente conocerá de la garantía del *Habeas Data* la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tendrá la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y la propia imagen. Los titulares de los órganos jurisdiccionales no podrán desechar la acción de *Habeas Corpus* o Exhibición Personal e igualmente tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad y a la seguridad personal. En ambos casos, los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones constitucionales, incurrirán en responsabilidad penal y administrativa. Las autoridades que ordenaren y los agentes que ejecutaren el ocultamiento del detenido o que en cualquier forma quebranten esta garantía incurrirán en el delito de detención ilegal».

El artículo 183 de la Constitución hondureña prosigue «el Estado reconoce la garantía de amparo. En consecuencia toda persona agraviada o cualquiera otra en nombre de esta, tiene derecho a interponer recurso de amparo: 1. Para que se le mantenga o restituya en el goce o disfrute de los derechos o garantías que la constitución establece; y 2. Para que se declare en casos concretos que un reglamento, hecho, acto o resolución de autoridad, no obliga al recurrente ni es aplicable por contravenir, disminuir o tergiversar cualesquiera de los derechos

reconocidos por esta Constitución. El Recurso de Amparo se interpondrá de conformidad con la Ley».

LA ACCIÓN CONSTITUCIONAL DEL *HABEAS DATA*

La norma constitucional reconoce el *Habeas Data* como garantía constitucional exhibitoria de datos de la persona humana y de sus bienes, pudiendo ser promovida únicamente por la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados; a la que se le reconocen los derechos de acceso, rectificación y cancelación, tal y como podría reconocerse en otras normas de otros países, como los reconocidos en la Ley Orgánica española, al establecer que si fuere necesario, podrán actualizar, rectificarla y-o enmendar la citada información; tal y como se desprende del Decreto Legislativo N.º 381-2005, mediante el que se reformó el Capítulo I, del Título IV de la Constitución de Honduras, donde se reconoce la garantía del *Habeas Data:* «que toda persona tiene el derecho a acceder a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla.»

La acción se constituye como un mecanismo procedimental de aplicación inmediata por las autoridades jurisdiccionales hondureñas, encaminada a paralizar y evitar cualquier violación a los de las personas. La Constitución hondureña al hacer un listado cerrado de supuestos, descarta la posibilidad que en otra clase de derechos y libertades constitucionales pueda ser posible utilizar este mecanismo procesal.

La acción del *habeas data* es una acción de trámite no oneroso y expedito, que puede ser ejercitada por cualquier persona que se vea afectada en el tratamiento de sus datos, sin necesidad de abogado o representante judicial, pudiendo ser ejercitada de forma verbal o por cualquier medio de comunicación. Conocerá de las acciones de *habeas data* la Sala Constitucional de la Corte Suprema de Justicia.

LEGISLACIÓN HONDUREÑA RELACIONADA

La Ley de Transparencia y Acceso a la Información Pública (Decreto número 170-2006) recoge en su artículo 2 entre sus objetivos, garantizar el ejercicio del derecho que tienen los ciudadanos a participar en la gestión de los asuntos públicos; promover la utilización eficiente de los recursos del Estado; hacer efectiva la transparencia en el ejercicio de las funciones públicas y en las relaciones del Estado con los particulares, garantizar la protección, clasificación y seguridad de la información pública y el respeto a las restricciones de acceso en los casos de información clasificada como reservada por las entidades públicas conforme a esta ley, información entregada al Estado por los particulares, en carácter de confidencialidad y los datos personales confidenciales, entre otras.

La Ley hondureña de transparencia en su Capítulo V hace referencia al tratamiento de los datos personales y el reconocimiento de la garantía del *habeas data,* así como la prohibición de entrega de información cuando pueda conllevar discriminación o causar daños o riesgos patrimoniales o morales a las personas. Del texto normativo deducimos que el acceso a los datos personales sólo se podrá realizar por orden judicial o a petición del propio interesado, representantes o sucesores.

Obliga la norma al poder ejecutivo, legislativo y judicial, así como a las instituciones autónomas, municipalidades y otros órganos e instituciones del Estado, a las Organizaciones No Gubernamentales, Organizaciones Privadas de Desarrollo y a aquellas personas físicas o

jurídicas que a cualquier título reciban o administren fondos públicos, cualquiera que sea su origen, nacionalidad.

A tenor de la citada norma, se entiende por dato personal confidencial, aquellos relativos al origen étnico o racial, características físicas, morales o emocionales, domicilio particular, número de teléfono particular, dirección electrónica particular, participación o afiliación a una organización política o ideológica, creencias religiosas o filosóficas, estados de salud físicos o mentales, el patrimonio personal o familiar y cualquier otro relativo al honor, la intimidad personal familiar o la propia imagen.

En este sentido dichas entidades han mantener subsistemas con suficiente soporte humano y técnico, que permitan la sistematización de la información, así como la prestación de un servicio de consulta y acceso por las personas, designando un Oficial de Información Pública como responsable de dichos subsistemas, formando en el espíritu de la Ley a los empleados y personas que accedan a la información o la traten por razón de su trabajo.

La Ley contempla un sistema de infracciones y sanciones asociadas, entre las que se encuentran no proporcionar de oficio o negarse a facilitar la información pública en el tiempo estipulado u obstaculizar su acceso; copiar, captar, divulgar o comercializar la información reservada; eliminar o alterar la información pública o reservada sin seguir los procedimientos de depuración establecidos; negarse a rectificar, actualizar o eliminar información falsa referente a datos personales confidenciales contenidos en cualquier archivo, registro o base de datos de las organizaciones e instituciones obligadas por la ley.

La Ley de Justicia Constitucional de Honduras, recoge en su Capítulo II la acción de exhibición personal y de *habeas data:*

Artículo 13

«El Estado reconoce la garantía de *habeas corpus* o exhibición personal, y de *habeas data*. En consecuencia en el *Habeas Corpus* o Exhibición Personal, toda persona agraviada o cualquier otra en nombre de ésta tiene derecho a promoverla; y en el *habeas data* únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados de la siguiente manera: (…) 2.) El *Habeas Data*. Toda persona tiene el derecho a acceder a la información sobre si misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla. Únicamente conocerá de la garantía de *habeas data* la Sala de lo Constitucional de la Corte Suprema de Justicia.»

Para garantizar el derecho a la privacidad, intimidad y el honor de las personas, así como mantener los datos personales actualizados y el correcto tratamiento de la información, aquellos que se aparezcan en el listado de morosidad de la Central de Información Crediticia hondureña, sin que medie justificación, pueden invocar el *habeas data* financiero, mediante el cual se reconoce el derecho personal de modificación o rectificación de información incorrecta o falsa.

Mediante la garantía del *habeas data* financiero, el ciudadano podrá conocer quien está reportando los datos a la Central de Información Crediticia y el derecho a recibir el finiquito de pago de su obligación en un plazo máximo de 10 días hábiles.

En otro ámbito se debe recordar que el Código de Ética del Colegio Médico de Honduras, tomando la Ley Orgánica del Colegio Médico de Honduras en el Capítulo I, Artículo 3, inciso c), reconoce «una función ética, cual es, la de mantener incólume la integridad de la moral profesional y el prestigio del gremio que la sustenta» y en el artículo 6 establece los entre sus fines aplicar y propender reformas a las normas de ética profesional; en su artículo 14 al referirse al secreto médico afirma que «se entiende por secreto médico al acto de salvaguardar la información que por razón del ejercicio profesional, llegue al conocimiento del médico en la

relación médico paciente y su contexto, ya sea porque le fue confiada, o porque la observó o la intuyó. Esta información no debe ser compartida salvo previo consentimiento del paciente, por daño al mismo o a terceros».

En su artículo 16 el citado Código establece que «el médico tiene el deber de exigir a su equipo de trabajo absoluta discreción y observación escrupulosa del secreto médico». En relación al tratamiento automatizado de la información el artículo 18 dispone que «cuando se emplean sistemas de informática médica, estos no deben comprometer el derecho del paciente a la intimidad, sin su consentimiento.

En relación a las sanciones, el Reglamento de Sanciones del Colegio Médico de Honduras en su artículo 43 reconoce que el secreto es un deber inherente a la profesión misma que exige el interés público, la seguridad de los enfermos, la honra a la familia, la responsabilidad del médico y la dignidad del arte, estableciendo una sanción en caso de violación del mismo de mil lempiras la primera vez y suspensión del ejercicio profesional hasta por tres meses en caso de reincidencia.

UNA MIRADA AL FUTURO

En 2014 se conocía y comenzaba su socialización por parte del Instituto de Acceso a la Información Pública hondureño, el Anteproyecto de Ley de protección de los datos personales y accesión de *habeas data,* elaborado por el Dr. Lester Ramírez Irías.

El Anteproyecto toma como base la Resolución 45/95 Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales de la Organización de Naciones Unidad, la Directiva Europea 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, así como la Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad y de los datos de carácter personal de la Red Iberoamericana de Protección de Datos, así como el análisis comparado de la normativa existente en Colombia, Costa Rica, España, México y Uruguay.

El documento consta de once Títulos en los que se abarcan las disposiciones generales, los principios y derechos para la protección de datos personales, los procedimientos para hacer efectivos los derechos, los deberes de los responsables, la seguridad de los datos, la transferencia de datos, disposiciones sectoriales, mecanismos de vigilancia y sanción, la acción de *habeas data* y cánones.

Se establece que futura norma será de aplicación a todos aquellos datos personales registrados en bases de datos automatizadas o manuales, de organizaciones del sector público y privado, excluyendo las bases de datos mantenidas por personas naturales en el ejercicio de actividades personales o domesticas, las que tengan por objeto la seguridad pública, defensa, seguridad del Estado, materia penal e investigación de delitos, así como las creadas por leyes especiales y los archivos y datos de información periodística.

El Anteproyecto recoge las definiciones de aviso de privacidad como el documento físico, electrónico o en cualquier otro formato generado por el Responsable de Tratamiento que es puesto a disposición del Titular, previo al tratamiento de los datos; base de datos, como aquel conjunto organizado de datos personales que sea objeto de tratamiento o procesamiento, automatizado o manual, cualquier que sea la modalidad de su elaboración, organización o acceso. Se define dato personal como cualquier dato relativo a una persona natural identificada o identificable; consentimiento como toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el Titular consienta el tratamiento de datos personales que le concierne; entre otros conceptos.

Se recogen en el artículo 4 del Anteproyecto los principios para la protección de datos personales: lealtad y legalidad, exactitud, finalidad, acceso a la información, consentimiento, no discriminación, seguridad y responsabilidad.

En relación a los derechos de las personas frente a la recolección de sus datos, se establece que el Titular deberá ser informado, previamente de forma expresa, precisa e inequívoca mediante un aviso de privacidad.

El aviso de privacidad deberá contener, al menos:

— La identidad y domicilio del Responsable que recoge los datos.

— La finalidad del tratamiento y posibles destinatarios.

— Las opciones y medios que el Responsable ofrezca a los titulares para limitar el uso o divulgación de los datos.

— Las consecuencias de proporcionar datos o de la negativa de hacerlo o su inexactitud.

— Las transferencias de datos que pudieran realizarse.

— Los medios para ejercitar los derechos de acceso, rectificación, eliminación u oposición.

Se establecen como excepciones al consentimiento previo del titular:

— Cuando los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.

— Se recaben para el ejercicio de funciones propias del Estado o en virtud de una obligación legal.

— Se trate de listados cuyos datos se limiten en el caso de personas naturales a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento.

— Deriven de una relación contractual, científica o profesional del Titular de los datos y sea necesario para su desarrollo o cumplimiento.

— Se realice por personas naturales o jurídicas, privadas o públicas o su uso exclusivo sea personal o doméstico.

El Anteproyecto reconoce cuatro derechos a las personas sobre sus datos: acceso, rectificación, eliminación y oposición, además del derecho referente a la transferencia de datos y el derecho de indemnización.

El artículo 14 del Anteproyecto establece una serie de excepciones a los derechos para la protección de los datos personales: la seguridad del Estado, la seguridad y el ejercicio de la autoridad pública, la prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología de los profesionales, se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento, el funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas, la adecuada prestación de servicios públicos y la eficaz actividad ordinaria de la Administración, por parte de las autoridades públicas.

Se recoge entre las obligaciones del Responsable del Tratamiento elaborar un Manual de políticas y procedimientos, así como la implementación y su inscripción ante el Instituto de Acceso a la Información Pública. Deberá adoptar las medidas de seguridad para garantizar la seguridad de los datos personales y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado.

En este sentido no se podrán registrar datos en bases de datos que no reúnan las condiciones que garanticen dicha seguridad, y que no cuenten con mecanismos de seguridad física y lógica.

El Anteproyecto establece categorías especiales de datos, entre los que se incluye los datos sensibles, como aquella información que revele el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, así como los relativos a la salud, vida sexual y datos biométricos, entre otros. También se establecen criterios sobre el tratamiento de datos relativos a las telecomunicaciones y los relativos a bases de datos con fines publicitarios.

Se establecen dos tipos de bases de datos, atendiendo a la naturaleza del Responsable: titularidad pública y privada, en ambos casos se registraran ante el Instituto de Acceso a la Información Pública y Protección de Datos Personales.

El Instituto será el responsable de promover y garantizar el derecho fundamental de protección de datos personales y ejercer la vigilancia para garantizar el tratamiento de los datos, respetando los principios, derechos, garantías y procedimientos previstos en el Anteproyecto, conforme al artículo 45 del mismo.

Se creará a estos efectos la Gerencia de Protección de Datos Personales, que entre sus funciones, velará por el cumplimiento de la legislación, realizará las investigaciones, de oficio o a instancia de parte y ordenará las medidas necesarias para hacer efectivo dicho derecho, conocerá y resolverá los procedimientos relativos a protección de datos, podrá disponer el bloqueo temporal de datos cuando exista riesgo de vulneración de los derechos fundamentales de las personas, administrará el Registro Nacional de Protección e Datos.

En el Registro Nacional se inscribirán las bases de datos gestionadas por entidades públicas y privadas, las autorizaciones recogidas en el Anteproyecto, los manuales y procedimientos que elaboren e implementen los Responsables y los datos relativos a bases de datos que sean necesarios para el ejercicio de derechos de acceso, rectificación, eliminación y oposición.

Se establece la creación de un Consejo Consultivo de Protección de Datos. El Anteproyecto se completa, además, con un régimen de infracciones y sanciones clasificadas en leves, graves y muy graves, y el tratamiento de la acción constitucional del *habeas data,* así como los cánones relativos a la regulación y administración de bases de datos y comercialización de consulta.

4.6 PANAMÁ

Constitución Política

Artículo 29: La correspondencia y demás documentos privados son inviolables y no pueden ser ocupados o examinados sino por disposición de autoridad competente, para fines específicos y mediante formalidades legales. (…) se guardará reserva sobre los asuntos ajenos al objeto de la ocupación o del examen. Igualmente, las comunicaciones telefónicas privadas son inviolables y no podrán ser interceptadas (…).

ANTECEDENTES EN PANAMÁ DEL *HABEAS DATA*

La necesidad que Panamá tenía sobre una legislación clara y precisa en el tema de acceso a la información pública, como parte de una herramienta para el ejercicio de derechos constitucionales es de vital importancia para una sociedad democrática. Anterior a la ley existía una enorme duda ciudadana sobre la falta de transparencia en la administración pública, expresadas por medios de demandas de colectivos, entidades cívicas, gremiales, partidos políticos y otros sectores participativos de la vida nacional.

Ante este reclamo de parte de la sociedad civil —mayormente— se dio trámite a la ley, con el objetivo de devolver la confianza ciudadana en la administración pública a través del

establecimiento del derecho de acceso a la información como un derecho ciudadano y la instrumentación de recursos legales para hacer valer esos derechos, entre otros.

Podemos tener como premisa que la información que manejan los funcionarios del Estado pertenece a toda la comunidad, por ello, es y debe ser pública. La transparencia informativa respecto de los actos de las autoridades, además de ser un elemental derecho ciudadano, es la manera más eficaz para prevenir la corrupción.

La ley apareció en el momento indicado para consolidar la democracia y el Estado de Derecho en el país, buscando que la administración pública sea ente más transparente, participativo y accesible a los ciudadanos. Cuando la información se restringe aumentan los actos de corrupción, el endeudamiento irresponsable y los abusos de poder. Un gobierno que no tiene nada que esconder, es un gobierno responsable, honesto y democrático.

El tema de la normativa del *habeas data* en Panamá obedece también a una estrategia y cumplimiento de compromisos internacionales que tienen como uno de los tantos estandartes; la lucha contra la pobreza, pues la transparencia de toda la información económica del Estado, ayuda a la toma de decisiones certeras y fructíferas a los inversionistas.

El *habeas data* brinda la tutela efectiva de parte del Estado, a lo que en esta era de las tecnologías de la información Karla María Zaldívar[15] denomina «la identidad informática» de la persona humana, con miras a que se le «respete la integridad física, psíquica y moral», en la medida en que, como anota la citada jurista, «si bien no se le está «matando» o «hiriendo» en el sentido físico o natural de los términos, se le puede neutralizar y negar dicha integridad a partir de las posibilidades de control por medio electrónico que ofrecen los recursos informáticos».

Es importante recalcar que lo esgrimido por el profesor panameño Edgardo Villalobos[16], al decir que «(…) la intimidad siempre estuvo protegida en nuestro ordenamiento. El problema actual es si está protegida la violación a la intimidad a través de la informática».

Según el art. 26 de la Constitución Política panameña los derechos vinculados al derecho de la intimidad son el de la inviolabilidad del domicilio o residencia y el de la inviolabilidad de la correspondencia como de las llamadas telefónicas, contenido en el artículo de la Carta Magna. Según el jurista panameño Rigoberto González Montenegro, expresa citando a otro jurista; «Con la inviolabilidad del domicilio se busca, como expresa Pedro J. González-Trevijano, particularidad que por demás es aplicable en forma extensiva, a nuestro juicio, al de la inviolabilidad de la correspondencia y de las llamadas telefónicas, «preservar el carácter privado e íntimo de determinadas facetas y comportamientos de la existencia humana[17]».

Podemos citar una sentencia de la sala tercera de la Corte Suprema de Panamá que dice: «La intimidad de las personas y lo que dentro de esta área realicen los particulares debe quedar exento de las intromisiones o ingerencias (sic) externas, tanto de otros particulares como de la autoridad pública[18]».

Igualmente se refiere la siguiente sentencia del Pleno de la Corte Suprema, al decir:

«No se puede perder de vista que el Ministerio de Hacienda y Tesoro es el custodio legal de informaciones confidenciales de los contribuyentes en materia tributaria, lo que se establece a cargo

---

15 ZALDÍVAR, K. M.: «El derecho a la intimidad en la Era de la información», *Divulgación Jurídica,* año III, número 5, octubre de 1996, pp. 3-4.

16 VILLALOBOS, E. A.: *Introducción a la Informática. Informática jurídica y Derecho informático.* Panamá, 1997, p. 137.

17 RIGOBERTO GONZÁLEZ M.: *El* Habeas Data. Segunda edición, revisada y actualizada. Panamá 2002, p. 38.

18 Fallo de 19 de septiembre de 1994, de la Sala Tercera de la Corte Suprema, Registro Judicial de septiembre de 1994, p. 259.

del Ministro del ramo el deber de salvaguardar los datos referentes a la tributación de las personas naturales y jurídicas, cuidando, de manera especial, la debida reserva de la información que se maneja en esa entidad recaudadora (…)». «Hay aquí un claro compromiso constitucional de implementar medios que garanticen la debida protección del derecho que tienen los contribuyentes a su intimidad y a la confidencialidad de sus declaraciones tributarias (art. 29 C.N.)...[19]»

En base a lo anotado anteriormente, podemos decir que los antecedentes de *habeas data* en Panamá son la Constitución Política de Panamá y la jurisprudencia de la Corte Suprema de Justicia, que buscan el respeto a la privacidad del individuo, evitando que la misma sea considerada de dominio público y menos usada por el Estado —en situaciones ajenas a las que la ley permite por motivos de seguridad nacional— y los particulares.

MARCO JURÍDICO DEL *HABEAS DATA* EN PANAMÁ

En el 2002, la Asamblea Legislativa de Panamá dicta la Ley número 6, Ley sobre transparencia en la gestión pública, donde se incorporó al derecho positivo vigente la acción de *habeas data*. Esta normativa fue producto de un contexto social de la época, aunado a compromisos y tendencias internacionales en la materia de acceso a la información, por ello también se reguló el derecho de acceso a la información. El *habeas data,* esta en el Capítulo V, llamado «Acción de *Habeas Data*», y se comprende en los arts. 17, 18 y 19.

Según la normativa relacionada anteriormente, la acción de *habeas data* puede ser presentada por cualquier persona a la que no se le haya suministrado la información o dato personal solicitado o cuando se haya hecho de forma deficiente. Esta puede ser presentada por extranjeros o cualquier persona jurídica. Es necesario diferenciar que la acción cabe en los fácticos de que sea denegado el acceso a la información o en casos de datos personales, entendiéndose que en el caso de este último, solo el titular de los datos puede promover la acción. Esto lo explicaremos más adelante.

En la normativa se introducen el término de información confidencial, indicando que es todo tipo de información en manos de agentes del Estado o de cualquier institución pública que tenga relevancia con respecto a los datos médicos y psicológicos de las personas, la vida íntima de los particulares, incluyendo sus asuntos familiares, actividades maritales u orientación sexual, su historial penal y policivo, su correspondencia y conversaciones telefónicas o aquellas mantenidas por cualquier otro medio audiovisual o electrónico, así como la información pertinente a los menores de edad.

Por otro lado se conceptualiza como información de acceso restringido, aquella que está en manos de agentes del Estado o de cualquier institución pública, cuya divulgación haya sido circunscrita únicamente a los funcionarios que la deban conocer en razón de sus atribuciones, de conformidad con la ley. Acá entran la información que tenga que ver con la seguridad nacional, manejada por los cuerpos de seguridad, etc.

Por ello podemos entender que la acción de *habeas data* no prosperará cuando se trate de información confidencial solicitada por un tercero o en caso de información de acceso restringido.

Por otro lado podemos ver que la acción del *habeas data* contempla dos supuestos para prosperar «el derecho de acceso a la información» y «la información o dato personal reclamado».

---

[19] Fallo de 11 de julio de 1997, del Pleno de Corte Suprema, Registro Judicial de julio de 1997, p. 113.

Podríamos ubicar «el derecho de acceso a la información» que se refiere a la información de carácter general y pública, que está en manos del Estado. Esta debe ser de acceso de cualquier persona, y debe ser suministrada sin justificación o motivación alguna.

En el caso de «la información o dato personal reclamado» es la que incumbe a una sola persona, por ser una información o dato personal, lo que se limita acá es que tenga acceso cualquier otra persona.

En la ley 6 de 2002 expresa y a lo que acabamos de referirnos, el autor Rigoberto González M, en concordancia con Óscar Puccinelli[20] esgrime que hay dos clases de *Habeas Data;* el *habeas data* «tradicional» o «propio», que busca menguar los daños poder informático sobre los derechos individuales de cada persona» y el *habeas data* «no tradicional» o «impropio» que se refiere a tutelar y regular la colección y tráfico de información sobre los individuos. Dicho de otra manera, podemos decir que el *habeas data* propio se tutela el acceso a la información o dato personal de reclama, por ser de su incumbencia. En cambio el *habeas data* impropio enviste de facultad al individuo de solicitar el acceso a la información de carácter público.

Por ello se puede decir que el *habeas data* procede cuando haya una negativa de parte del funcionario o el responsable del registro ante la solicitud de la información de carácter público o de carácter personal. Así mismo, cuando sea suministrada de manera incompleta o insuficiente. También cuando la información suministrada no sea exacta o falsa.

La acción de *habeas data* se interpondrá contra el titular o responsable del registro, archivo o banco de datos —sea este informático o no—, o contra el custodio o responsable del manejo de la información en caso de ser empresa privada que prestan o suministran servicios públicos con carácter exclusivo.

El artículo 18 de la Ley 6 de 2002, dice que la acción de *Habeas Data* será competencia de los Tribunales Superiores que conocen de la acción de Amparo de Garantías Constitucionales, cuando el funcionario titular o responsabilidad, registro o archivo o banco de datos, tenga mando y jurisdicción a nivel municipal o provincial. Cuando el titular o responsable del registro, archivo o banco de datos tenga mando y jurisdicción en dos o más provincias o en toda la República, será de competencia del Pleno de la Corte Suprema de Justicia.

La acción de *habeas data* no esta revestida de ninguna formalidad, busca de manera sencilla lograr la tutela de derechos constitucionales a los individuos. Esta falta de formalidad tiene amparo constitucional en el artículo 212 de la Constitución que establece que las leyes procesales que se aprueben se inspirarán, entre otros principios, en el de la ausencia de formalismos dando especial atención a la ley sustantiva.

Podemos concluir que con esta normativa una vez más Panamá marca una referencia legislativa proteccionista de las garantías individuales de las personas, sin importar su situación migratoria, pues se viene a fortalecer y ampliar los mecanismos de protección de los derechos fundamentales, marcando de esta forma un sólido compromiso con la apertura a la inversión y la democracia.

---

[20] PUCCINELLI, O.: *El* Habeas Data *en Iberoamérica.* Edit. Temis, 1999, p. 22.

5. OTROS PAÍSES Y EL TRATAMIENTO DE LA PROTECCIÓN DE LOS DATOS PERSONALES

5.1 CUBA

BIEN JURÍDICO PROTEGIDO

Se tiene la dualidad propia del derecho informático, se protege la información y los medios electrónicos como algo intrínseco a la información, en su calidad de medio de comunicación.

Es la información la que se protege pero sin hacer hincapié en la importancia de la misma, tal como se verá posteriormente en el acápite de *habeas data,* dentro del Estado de Cuba no se ha logrado legislar la complejidad que abarca la información como bien jurídico, al no haber sido elevado como derecho constitucional.

HABEAS DATA

El *habeas data* hace referencia a una acción constitucional que nos permite acceder a bases de datos con el fin de realizar correcciones sobre datos que dañen a nuestra persona, esta acción se encuentra reconocida dentro de la Constitución Política del Estado de aquellos países que hayan elevado a grado constitucional estos derechos.

Cuba no ha incorporado hasta la fecha, dentro de su constitución política del estado, la acción tutelar del *habeas data,* esto no significa que no exista medio jurídicos para proteger la información de su población, sin embargo cuando una constitución no otorga una acción de esta índole, si representa cierta desventaja dentro de lo que se conoce como protección de datos personales.

Es la Constitución Política del Estado, el origen de toda normativa, es la base y el marco, para desarrollar leyes especiales orientadas a tutelar los bienes jurídicos, es en este sentido, la razón por la cual se debería contemplar de manera constitucional la acción de *habeas data,* no solo por su misma finalidad que es la de conocer, rectificar, eliminar, modificar, información en desconocimiento o perjuicio de su titular, sino que una vez dentro de la Constitución Política del Estado, es cuando se reconoce este tipo de acciones y gracias a ello se deja un espacio abierto para que sea posible la elaboración de mecanismos especializados para tutelar estos bienes.

Dentro de la información existen bienes jurídicos anexos, estos llegan a ser desde la imagen hasta la privacidad, el *habeas data* es un mecanismo para lograr la autodeterminación informática, es decir es una acción constitucional que nos permite subsanar nuestra imagen, privacidad, honra, que ha sido vulnerada, por lo que se debe entender que al no darle a los ciudadanos la garantía que ofrece el *habeas data,* se les está privando la oportunidad de reclamar ante la injusticia de quienes usan sus datos sin consentimiento, dándoles un destino comercial el mismo que a su vez vulnera la privacidad de los cubanos usuarios de internet.

LEYES CON RELACIÓN A LA PROTECCIÓN DE DATOS

Es reflejo de la falta de un marco constitucional en materia de protección de datos, que las leyes vigentes en Cuba respecto a los datos, no sean las suficientes para abarcar una tutela adecuada.

Resolución del Ministerio del Interior 18 de noviembre 1996, confidencialidad, integridad y disponibilidad. Esta normativa establece directrices de implementación de un sistema de medidas administrativas, organizativas, físicas, técnicas y legales con miras a la confidencialidad, integridad y disponibilidad de todas las actividades concernientes en el uso de las tecnologías de la información.

Ley 199 de seguridad y protección de la información oficial, dictada por el Consejo de Estado en noviembre 1999. Esta normativa por otro lado la que regula mecanismos para la seguridad y protección de la información oficial aplicable a los órganos, organismos, entidades o a cualquier otra persona natural o que reside en Cuba. De alguna manera esta normativa se ocupa de regular los aspectos relevantes al hardware como ser la protección criptográfica, al igual que establece de manera expresa que la información no sea divulgada de manera no autorizada.

Podría deberse a su realidad social, posiblemente los daños a la información permanecen aun en aquella cifra oculta por falta de denuncia, o puede darse porque en los hechos las vulneraciones son mínimas, sin embargo, el derecho nos ha demostrado que la normativa siempre es escasa ante la realidad social presente en cada Estado.

5.2 EL SALVADOR

Constitución de la República de El Salvador

Artículo 2: Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

BIEN JURÍDICO PROTEGIDO

El Salvador no cuenta con la acción constitucional para la autodeterminación informática, es decir que el *habeas data* no es una acción reconocida para los ciudadanos de este estado, sin embargo motivado por la necesidad de garantizar de manera constitucional los derechos que son vulnerados en relación a la falta de protección de datos, se emitió jurisprudencia por su Corte Suprema de Justicia, el mismo que logra subsanar esta falta en cuanto a la protección de datos en su Sala Constitucional.

JURISPRUDENCIA SALVADOREÑA

Sentencia 934-2007 El Salvador INDATA *vs*. INFORNET

Esta sentencia nos señala al accionante de un amparo constitucional, siendo INDATA en representación de un grupo de personas quienes indican que INFORNET S.A ha estado recolectando, manipulando y comercializando datos personales de 4 millones de salvadoreños, y esto sin permiso o autorización de los titulares, fundamentan que INFORNET S.A ha incurrido en acciones inconstitucionales al momento de violentar intereses colectivos al igual que el derecho a la autodeterminación informática.

Esta sentencia constitucional, es por demás interesante y enriquecedora para el desarrollo posterior de la normativa en el Salvador, puesto que dentro de su fundamentación para el fallo,

se puede observar como separa el derecho a la intimidad y el derecho a la protección de datos privados, como dos bienes jurídicos tutelados distintos.

La protección de la información no se limita solo a si esta vulnera la privacidad del usuario.

«Al contrario el ámbito de protección de este derecho no puede limitarse a determinado tipo de datos –sensibles o íntimos–; lo decisivo es la utilidad y el tipo de procesamiento que de los mismos se haga. Es decir, la vulneración al derecho en mención depende de la finalidad que dicha actividad persiga y de los mecanismos de control que al efecto se prevean.

Así, determinar cuánto riesgo existe sobre el mal uso de la información personal, no dependerá sólo del hecho de que se toquen asuntos íntimos; fijar el significado o valor de un dato con respecto a la autodeterminación informativa, requiere conocer el contexto en que se utiliza o se pretenda utilizar. Por ello, el grado de sensibilidad o intimidad de las informaciones ya no depende únicamente de si se afecta o no la esfera íntima; hace falta, más bien, conocer la relación de utilización de un dato para poder determinar sus implicaciones en el individuo.»[1]

Dentro de este extracto de la sentencia, se observa cómo se introduce el principio de aviso, mediante el que posea una base de datos debe ser claro en sus políticas de uso de datos personales, indicando que destino o tratamiento realiza con la información.

En cuanto al fallo de esta sentencia constitucional, se da lugar al amparo solicitado por INDATA, de igual manera la corte ordena a INFORNET S.A, que permita a los accionantes el acceso a la base de datos para rectificar, modificar o eliminar la información que pueda lastimarlos, por último se obliga a INFORNET que no trate los datos con terceros si es que los titulares de la información no han aceptado estas acciones.

LEYES RELACIONADAS A LA PROTECCIÓN DE DATOS

Ley de Bancos. Decreto Legislativo N. 697. En su art. 133 dentro de sus potestades señala que podrá compartir bases de datos de clientes. Es decir tiene el permiso para disponer información económica financiera respecto de sus clientes con las otras entidades información, con la prohibición de revelar el secreto bancario. En este caso, es la normativa la que se encarga de anunciar el principio de aviso para este sector.

Ley Protección al Consumidor. Decreto Legislativo N.º 166. 08/09/2005. En su artículo 21 obliga a las instituciones que prestan servicios de información, a que colaboren y faciliten a los usuarios, o para fines de esta ley consumidores, a su autodeterminación informática relacionada con los servicios prestados. Es un gran avance en cuanto a normativa de protección de consumidor, es normal ver en otras normativas que se crea una ley específica para protección de datos, sin embargo en El Salvador, se ha establecido como un derecho inherente a la relación de compra y consumo.

Reglamento General de Ley Penitenciaria. En su art. 19 establece en que casos los centros penitenciarios por medio de su secretaria podrán facilitar el acceso a datos de los internos cuando estos por escrito así lo convengan y a jueces o al ministerio público, se les facilitara el acceso a esta información sin necesidad del consentimiento del titular, bajo el entendido de que estos órganos de administración de justicia y coadyuvante, requieren de la información para cumplir con sus labores públicas.

Esta disposición enmarca de forma clara el equilibrio entre dos derechos que son el acceso a la información y el de privacidad, puesto que si bien todos tenemos el derecho a acceder a la

---

[1] Sentencia 934-2007 El Salvador INDATA *vs*. INFORNET, Sala de lo Constitucional de la Corte Suprema de Justicia, San Salvador.

información esto debe ser con justa causa, como la es del ministerio público o jueces, cuando deben ejercer ese derecho para lograr cumplir con sus labores.

El art. 20 hace una distinción entre los datos que se facilitaran y los que ya incurren en otra esfera del titular, cuyo contenido de los datos no son necesarios para fines mayores y pueden vulnerar al dueño de la información, este tipo de datos íntimos, hacen referencia a las opiniones política, religiosas y de orientación sexual.

Lo contradictorio con este artículo, es el hecho de que si bien hace una diferencia con este tipo de información, y por supuesto indica el mecanismo para poder acceder a ella, el modo de disponer de estos datos, se plasma de manera amplia dando poca protección a los datos íntimos, claro es el ejemplo de desprotección por escritura abstracta cuando indica que pueden ser difundidos cuando por razones de interés general lo disponga una ley, es a criterio del escritor, un permiso a futuro que podría dar un fácil acceso a datos íntimos de internos penitenciarios.

En el art. 21 indica el procedimiento para la rectificación de datos personales, siguiendo la lógica de la autodeterminación informática.

En su art. 22 garantiza la protección de los datos, por parte de los que se encargan de tratarlos, incluyendo tiempo posterior de dejar de desempeñar un cargo en la institución, los administradores se ven imposibilitados de difundir dicha información.

5.3 VENEZUELA

Constitución de la República Bolivariana de Venezuela

> Artículo 28: Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados (…) conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas.

BIEN JURÍDICO PROTEGIDO

Es importante reconocer dentro de la Constitución Política del Estado, la autodeterminación informática, esto para que a momento posterior las normativas especificas cuenten con una base legal en que sustentarse, de igual manera se debe valorar el reconocimiento constitucional del *habeas data,* puesto que la Constitución Política del Estado, posee una naturaleza política y no así jurídica, por lo que lo que dicta una Constitución, es lo que dicta la realidad del Estado, su forma de organizarse y de fluir sobre cada esfera de sus habitantes, por lo que el reconocimiento del *habeas data* dentro de una Constitución Política del Estado, significa la aceptación y respeto primordial ante este aspecto con los ciudadanos.

Venezuela dentro del art. 28 de su Constitución reconoce la autodeterminación informática, en amplitud para conocer, modificar y eliminar todos los datos concernientes a su titular, depositados en cualquier base de datos o registro. Esta constitución es amplia y otorga facilidad para ejercer la autodeterminación informática en su totalidad, al no hacer una diferencia entre base de datos pública y privada.

La información y los datos pueden encontrarse en imágenes, y la divulgación de estas puede generar perjuicio en la honra y reputación, por lo que es menester mencionar y elevar a grado

constitucional estos derechos, el art. 60 reconocer estos derechos, junto a la protección de la vida privada, intimidad, confidencialidad y reputación.

La necesidad de proteger este ámbito de los ciudadanos, avanza hasta el punto, de otorgarle al Defensor del Pueblo la legitimidad de interponer la Acción de Amparo, esto se reconoce en el art. 281, cuando se habla de sus competencias. Estos tres aspectos constitucionales en referencia a la autodeterminación informática, son muestra de los resultados obtenidos por la comprensión e intención del estado para proteger los datos de sus ciudadanos.

JURISPRUDENCIA VENEZOLANA

Sala Constitucional Sentencia n.º 1318, de fecha 04-08-2011

Siendo el presente un caso interesante para analizar, y no a causa del fallo, sino por los principios en materia de protección de datos, que se han reconocido dentro de la fundamentación.

La acción versa sobre la petición de declarar inconstitucional el artículo 192 del Decreto n.º 1.526 con fuerza de Ley de reforma de la Ley General de bancos y otras instituciones financieras, esto porque «han venido utilizando la información contenida en dicho sistema en detrimento de los deudores, en el sentido de que los entes crediticios distintos a aquél que estableció la relación jurídica con el beneficiario del crédito, manipulan sus datos de identificación, el resumen de su deuda y su situación de morosidad, a los fines de calificarlo según su situación crediticia y establecer su capacidad de pago, estigmatizándolo como de alto o bajo riesgo para asumir nuevas obligaciones crediticias»

En la sentencia no se logra modificar el contenido, puesto que antes del fallo, se deroga por normativa vigente antes de decidir sobre la controversia, es por esta razón que no es trascendental el resuelve del caso, pero si algunos elementos que se tocan en la fundamentación.

El principio de voluntad de las partes, es un principio que se lo establece con carácter vinculante, este principio consiste en la necesaria existencia previa de consentimiento para el uso de la información.

Se desarrolla de igual manera el principio de finalidad y cualidad, mediante el cual, el recolector de datos debe informar cual es el objetivo de dicha recolección de información, y sus actos deben ser acordes a la información recolectada.

Siendo estos dos principios innovadores dentro de la normativa de la República de Venezuela, es necesario hacer hincapié en su inclusión gracias a la jurisprudencia.

LEGISLACIÓN RELATIVA A LA PROTECCIÓN DE DATOS

Ley de registro de antecedentes penales del 3 de Agosto de 1979. Esta normativa en su art. 8 prohíbe la solicitud de antecedentes penales, cuando sea por razones de contratación laboral.

Esta ley obedece a un tema de mayor reincidencia como lo es la aceptación social en cuanto a ex privados de libertad, las más avanzadas teorías de criminología critica, indican que la cárcel no reforma, es más tiende a marcar a los individuos, dificultándoles su posterior reinserción en la sociedad, por lo que el proteger este tipo de información para evitar el hostigamiento a las personas es un avance en los derechos fundamentales de los ciudadanos.

Ley sobre Protección a la Privacidad de las Comunicaciones del 16 de Diciembre de 1991. Esta normativa protege de manera específica la intercepción de comunicaciones privadas, o la interrupción de esta, esto mediante simple intercepción o con la instalación de software

especializados, los que incurran en este acto deberán cumplir una pena de 3 a 5 años de prisión por incumplimiento a la presente ley.

Se establece el procedimiento de solicitud judicial para poder acceder a las comunicaciones privadas, algo que no es de mayor novedad, puesto que normalmente este tipo de procedimientos figura en los códigos de procedimiento penal.

Ley Orgánica para la Protección del Niño y del Adolescente del 10 de Febrero de 1998. Esta normativa enmarca direccionado para los menores de edad, la inviolabilidad de sus derechos constitucionales, honor, reputación y propia imagen, vida privada e intimidad de la vida familiar.

Indica prohibiciones para la divulgación de imágenes y datos de menores de edad por cualquier medio, y extiende a la divulgación de documentos, actos y declaraciones de manera total o parcial. Este tipo de normativa es generada por su constitución en correlación a los derechos de los niños y el derecho a la imagen, el cual muchas veces es violentado por la fragilidad del sujeto pasivo.

Es mediante esta normativa que se abre espacio para que las ONGs interesadas en la materia puedan generar cultura de protección de datos para los adolescentes quienes aún no han aprendido a navegar seguros, y dejan imágenes al alcance de sujetos con malas intenciones.

Ley Especial contra Delitos Informáticos del 30 de Octubre de 2001. Cuando hablamos de delitos informáticos, se debe entender que lo que se prioriza es la información del sujeto pasivo, pero para poder proteger este tipo de información es necesario darle tutela a los medios informáticos, sin la necesidad de darles el valor de bienes, sino de medios donde se guarda la información y datos, si cayéramos sobre la lógica de que los delitos informáticos protegen cualquier medio electrónico, no habría diferencia entre estos delitos y los que se cometen contra la propiedad privada.

Mediante su artículo 6 se penaliza el acceso indebido o intercepción indebida a un sistema informático de comunicación, lo que se pretende salvaguardar mediante penas, es la importancia de la información contenida en ese sistema informático.

En su artículo 11 tipifica el espionaje informático, detallando que aquel que de manera ilegítima obtenga o divulgue datos contenidos en un sistema electrónico, incurrirá en una pena de 3 a 6 años.

Estos son los dos delitos que de manera concreta se refieren a los datos y su protección, los demás delitos tipificados en la ley penal, hacen mucha referencia al daño del sistema electrónico, lo cual es propio del estado actual del derecho informático y su expansión penal, en la que se castiga el daño a la dualidad del sistema y los datos.

El Decreto con fuerza y rango de Ley de la Función Pública de Estadística del 09-11-2001. Esta normativa tuvo gran reincidencia para proteger a los ciudadanos de las persecuciones políticas que se podrían dar, a causa del conocimiento de datos personales de los ciudadanos, el dato crítico era su afiliación política, que se quedaba registrada al momento de ser encuestados.

Este tipo de peligros concurren cuando por ejemplo en el año 2003 se convocó a un referéndum, y no existía ningún tipo de protección para los datos de los ciudadanos que hacían uso de este derecho. Es por ello que esta normativa protege los datos de los ciudadanos ante los funcionarios o sujetos que tengan acceso a este procedimiento de voto.

6. EQUILIBRIO ENTRE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS

Antes de analizar el concepto de acceso a la información pública, es conveniente mencionar lo que en términos generales entenderíamos como información pública, para ello y en palabras de Pulido Jiménez, la información pública es aquella que los órganos del Estado generan, obtienen, adquieren, transforman o conservan con motivo de su actuación, y de forma especial, la que documenta el ejercicio de sus facultades o su actividad.[1]

Ahora bien, los órganos del Estado tienen la obligación de generar, administrar y resguardar dicha información pública, pero no solo con la finalidad de facilitar las actividades gubernamentales, sino también con la finalidad de que los ciudadanos puedan tener acceso a la misma, ello ya que al final de cuentas las actuaciones de las autoridades, así como la información y documentación que generan forman parte de una serie de actividades que se llevan a cabo mediante el empleo de fondos públicos, los cuales provienen del ciudadano a través del pago de impuestos, derechos, aportaciones y demás formas mediante las cuales la ciudadanía realiza una aportación al Estado para que éste pueda llevar a cabo las actividades relacionadas con la administración pública.

Es por lo anterior, que se reconoce el derecho del ciudadano para que pueda acceder a la información pública gubernamental y además, a la de las personas que reciban aportaciones o apoyos relacionados con recursos públicos. En ejemplo de lo anterior tenemos una de las recientes reformas a la Constitución Política de México, por medio de la cual se estableció que «Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública…»[2].

Lo anterior es un gran paso, ya que no solo se reconoce como información pública la información de las dependencias de Gobierno, sino también de todos aquellos que reciban aportaciones derivadas de recursos públicos, ello como parte de la rendición y transparencia de las cuantas a la ciudadanía.

Es así, que llegamos al análisis conceptual del derecho de acceso a la información, para lo cual citamos a López Ayllón, quien menciona que el derecho a la información comprende tres facultades interrelacionadas: la de buscar (investigar), de recibir o difundir informaciones, opiniones o ideas[3]. En *lato sensu* viene a constituir una «prerrogativa fundamental» en donde

---

1 PULIDO JIMÉNEZ, M.: *El acceso a la información es un derecho humano,* tomo 2, serie: Ombudsman, México, 2006, p. 9.

2 Cámara de Diputados, «Constitución Política de los Estados Unidos Mexicanos», México, 2014, artículo 6, inciso A, fracción I. Tomado de http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm.

3 De esta formulación el citado autor señala que el derecho a la información consiste en que «cualquier individuo puede, en relación con el Estado, buscar, recibir o difundir –o no buscar, no recibir, ni difundir– informaciones, opiniones e ideas por cualquier medio, y que tal individuo tiene frente al Estado un derecho a que éste no le impida buscar, recibir o difundir –o no lo obligue a buscar, recibir o difundir– informaciones, opiniones e ideas por cualquier medio. Vid. López Ayllón, S. (2000). *op cit.*, p. 163.

toda persona posee el derecho a: atraerse información, a informar y a ser informado»[4]. Es decir, se está frente a una potestad o facultad que el Estado reconoce u otorga a sus gobernados[5].

De donde se desprende que, frente al acto concreto de una autoridad, debe establecerse la relación con el gobernado y sí este acto arbitrario vulnera directamente el derecho de informar o el de estar informado, se estará ante a un derecho fundamental —derecho a la libertad de información— y si se requiere de la implementación de una serie de medidas a través de la legislación ordinaria, se estará frente a uno de carácter social —derecho de acceso a la información pública—.

Ahora bien, nos podemos preguntan y en dónde se encuentra la relación entre este derecho a la información, respecto de la protección de datos personales. Ya que el primero habla de una apertura de la información y de una transparencia, mientras que el segundo se refiere a la protección de los datos personales, entendidos estos como «…toda información sobre una persona física identificada o identificable (el «interesado»);…»[6].

Sin embargo, tanto el acceso a la información como la protección de datos personales convergen en un punto, ello en el momento en el que muchos de los documentos e información pública que se encuentra en poder de los Estados u sujetos obligados contienen datos personales de los ciudadanos, razón por la cual es indispensable que el Estado en cuanto responsable de la información pondere entre su obligación de proporcionar y dar acceso a la información pública gubernamental, y su deber de proteger los datos personales contenidos en los documentos que obran en sus archivos o bases de datos.

De ahí que, la protección de datos personales, en un principio, al constituirse como un límite al derecho de acceso a la información y, dada la necesidad de proteger los datos personales de los ciudadanos, poco a poco hemos visto que en las legislaciones de diversos países iberoamericanos además de considerar el derecho de acceso a la información pública, se ha ido incorporando también la protección de datos personales.

Es así que poco a poco se han visto cambios no solo en la legislación, sino que además, se han observado en los criterios emitidos por las cortes o tribunales jurisdiccionales, en donde si bien se vela por el acceso de los ciudadanos a la información pública, sino también se vela porque las autoridades supriman la información o contenidos relacionados con los datos personales contenidos en la información pública.

Ejemplo de lo anterior tenemos algunos ejemplos de legislaciones o criterios en algunos de los países de Iberoamérica, como son:

España. Se establece que en los casos en los cuales la información solicitada contenga datos especialmente protegidos, como lo son los datos personales, el acceso a los mismos solo podrá ser autorizado cuando se cuente con el consentimiento expreso y por escrito del afectado, ello a menos que éste último hubiere realizado o manifestado de manera pública tales datos personales y con anterioridad a que se solicitase el acceso.[7]

---

4 Cabe destacar de los tres aspectos en donde a) el atraerse información, incluye las facultades de acceso a los archivos y documentos públicos; b) a informar, se incorporan las libertades de expresión y de imprenta; y, c) a ser informado en donde se establecen las facultades de recibir información objetiva y oportuna —enterarse de todas las noticias— con carácter universal —que la información sea para todas las personas sin exclusión alguna—. Vid. Villanueva, E. (2003). Derecho de Acceso a la Información Pública en Latinoamérica: Estudio Introductorio y Compilación. México. Universidad Nacional Autónoma de México.

5 Ídem.

6 Parlamento Europeo, «Directiva 95/46/CE, Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos», 2014, artículo 2, inciso b), tomado de http://www.acave.travel/sites/default/files/comunitario-Directiva%2095-46-CE.pdf.

7 Jefatura del Estado, «Ley 19/2013 de transparencia y acceso a la información pública y de gobierno», España, 2013, artículo 15. Tomado de https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf.

México. La Suprema Corte de Justicia del Estado Mexicano determino que «…es menester concluir que el derecho de acceso a la información no es absoluto y se encuentra limitado por los demás derechos consagrados en el orden jurídico nacional, entre otros, el derecho a la privacidad, el cual se tutela en ese mismo ordenamiento[8] al proteger los datos personales que tienen bajo su resguardo los órganos de la Federación e incluso en los diversos instrumentos internacionales…»[9].

Ecuador. En su legislación en materia de transparencia por una parte se establece que la información pública será todo documento en poder de las instituciones públicas, sea que se trate de documentos contenidos, creados u obtenidos por ellas, y que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.

Sin embargo, también se establece que se considera como ilegal el uso que se haga de la información personal, así como la divulgación de la información confidencial, entendida como tal la información pública personal, que no está sujeta al principio de publicidad.[10]

Así mismo, la protección de los datos personales se puede observar desde el objeto mismo de la norma, ya que se establece como uno de sus objetivos el garantizar la protección de la información personal en poder del sector público.

Nicaragua. Se establece expresamente que la información privada en poder del Estado no se considera de libre acceso público, en el entendido de que se entiende como información privada la que está compuesta por datos personales referidos a la vida privada y familiar, tales como salud, raza, preferencia política o religiosa, situación económica, social o familiar o su honra y reputación.[11]

Para finalizar, es importante destacar que el acceso a la información pública no solamente cobra importancia porque empodera al ciudadano y le da la facultad de conocer en qué y en donde están siendo invertidos los recursos públicos o respecto de las actuaciones de las autoridades.

Sino que sobre todo por el creciente incremento del uso de las tecnologías de información y comunicaciones, así como la rápida evolución que están teniendo, a nivel internacional se ha mencionado o reconocido la importancia de que los países reconozcan el acceso a la información pública.

Tal es el caso de la Convención Interamericana de Derechos Humanos, la cual desde el 2005 reafirmó en la resolución AG/RES. 2121 (XXXV-O/05) sobre el «Acceso a la Información Pública: Fortalecimiento de la Democracia»[12], que las personas tienen la libertad de buscar, recibir, acceder y difundir informaciones, así como el que pueden acceder a la información pública, ello como requisito indispensable para la democracia.

---

8 Constitución Política de los Estados Unidos Mexicanos.

9 Suprema Corte de Justicia de la Nación, Criterio 08/2006, «Información pública gubernamental. al interpretar lo previsto en la ley federal de transparencia y acceso a la información pública gubernamental así como en las disposiciones emanadas de ésta debe considerarse que dicho ordenamiento también tutela el derecho a la privacidad.», México, 2006.

10 Congreso Nacional de Ecuador, «Ley Orgánica de Transparencia y Acceso a la Información Pública», 2004, Ecuador, artículos 2, 5 y 6. Tomado de http://www.ecuadorestrategicoep.gob.ec/images/leytransparencia/LOTAIP.pdf.

11 Asamblea Nacional, «Ley de Acceso a la Información Pública», Nicaragua, 2007, artículos 1.º y 4.º inciso m). Tomada de http://www.oas.org/juridico/spanish/mesicic3_nic_ley621.pdf.

12 Comisión Interamericana de Derechos Humanos, AG/RES. 2121 (XXXV-O/05) sobre el «Acceso a la Información Pública: Fortalecimiento de la Democracia», 2005. Tomado de http://www.oas.org/es/sla/ddi/docs/AG-RES_2121_XXXV-O-05_esp.pdf.

Así como también, la Organización de Estados Americanos (OEA) reconoció la importancia del acceso a la información pública en la «Declaración De Santo Domingo»[13], ya que se declaró la importancia de la modernización del Estado mediante estrategias de gobierno electrónico, entre otros para mejorar la provisión de información a la población, así como para incrementar la transparencia y la rendición de cuentas.

Para finalizar el presente capítulo, es importante concluir que como se expuso en los párrafos anteriores, los derechos de protección de datos personales y de acceso a la información van muy de la mano. Sin embargo, la diferencia entre los mismos radica en el que el acceso a la información involucra el derecho a informar y a ser informado, es decir, por una parte las autoridades o sujetos obligados tienen el derecho y obligación de exhibir y dar a conocer cierta información relacionada con los actos que desempeñan, información que es dada a conocer mediante los esquemas conocidos como transparencia focalizada o de oficio, y por otra parte, las personas tienen también el derecho de solicitar información adicional a la publicada por los sujetos obligados, para lo cual, tienen el derecho de realizar las peticiones que a su derecho convengan.

Pero siempre velando por que la información que se ponga a disposición del público de manera oficiosa o cuando corresponda a una solicitud expresa de la ciudadanía, siempre se deberán de proteger los datos personales que obren en los documentos, bases de datos o demás información que constituya información pública.

---

13 Organización de Estados Americanos, AG/DEC. 46 (XXXVI-O/06) «Declaración de Santo Domingo: Gobernabilidad y Desarrollo en la sociedad del conocimiento», 2006, tomado de http://www.oas.org/36ag/espanol/DECSANTODOMs04.doc.

7. TRANSFERENCIAS INTERNACIONALES DE DATOS

Como otros tantos aspectos, las transferencias internacionales de datos (TID) son reguladas de forma distinta en aquellos países iberoamericanos que ya cuentan con una legislación destinada a la protección de los datos personales y/o la privacidad de los individuos.

Aunque las TID pueden ser definidas a partir de algunas características comunes, nos encontraremos con que en algunas jurisdicciones el carácter internacional de la transferencia dependerá del Estado o territorio de destino; que en ocasiones se denominan «comunicaciones» o «flujos»; que pueden o no estar sujetas a una autorización previa antes de poder ser efectuadas, o que su carácter internacional no depende de que los datos salgan, necesariamente, del territorio nacional del responsable.

Así por ejemplo, en España la comunicación de datos personales efectuada hacia un responsable ubicado en un Estado del Espacio Económico Europeo (EEE)[1] no se regula como TID, sino como una cesión de datos; mientras que la normativa comunitaria regula como TID la comunicación de datos hacia un encargado del tratamiento establecido en un «tercer Estado», e incluso ha dispuesto de cláusulas contractuales tipo para este tipo de transferencias.[2]

A partir de estas consideraciones previas, en el presente capítulo pretendemos sintetizar los conceptos, características y requisitos específicos que las legislaciones hasta ahora analizadas contienen en relación con las TID.

7.1 ANÁLISIS DE LEGISLACIONES

La comparación entre las definiciones legales (cuando existen) y los requisitos establecidos para poder llevar a cabo TID, permite comprobar que las legislaciones analizadas no regulan de forma homogénea este tipo de comunicaciones de datos personales. El siguiente análisis comparativo aborda los aspectos más relevantes al respecto.

7.1.1 PAÍSES CON LEGISLACIÓN ESPECÍFICA EN MATERIA DE PROTECCIÓN DE DATOS

Andorra

En este país, se considera «comunicación internacional de datos» «toda comunicación de datos, o todo acceso a los datos por parte de un prestador de servicios de datos personales,

---

1 Ver 94/1/CE, CECA: Decisión del Consejo y de la Comisión de 13 de diciembre de 1993 relativa a la celebración del Acuerdo sobre el Espacio Económico Europeo entre las Comunidades Europeas y sus Estados miembros, por una parte, y la República de Austria, la República de Finlandia, la República de Islandia, el Principado de Liechtenstein, el Reino de Noruega, el Reino de Suecia y la Confederación Suiza, por otra parte, en: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:31994D0001.
Cabe señalar que el acuerdo sobre el EEE fue firmado en 1992 entre los doce Estados miembros y los seis Estados miembros de la Asociación Europea de Libre Comercio (AELC), que eran por entonces Austria, Finlandia, Islandia, Liechtenstein, Noruega, Suecia y Suiza. No obstante, el acuerdo no entró en vigor hasta 1994, debido al rechazo de Suiza. En 1995, Austria, Finlandia y Suecia se adhirieron a la Unión Europea.

2 Ver 2010/87/: Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo [notificada con el número C(2010) 593] (Texto pertinente a efectos del EEE), en http://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1401799946706&uri=CELEX:32010D0087.

cuando los destinatarios de la comunicación o los prestadores de servicios estén domiciliados en el extranjero, o empleen medios de tratamiento de datos personales ubicados en el extranjero para la comunicación de los datos o para la prestación del servicio.»[3]

Requisitos:

1. Consentimiento del titular: Se aplican a las TID las reglas previstas en la normativa andorrana para la recogida y tratamiento de los datos personales. No hay una particularidad en cuanto a este requisito referido a las TID, salvo el hecho de que el consentimiento inequívoco del titular habilita «per se» una transferencia realizada a un país cuya normativa no garantice un nivel de protección adecuado y suficiente tal y como lo garantiza la legislación de Andorra.
2. Nivel de protección equivalente/adecuado en el destino: La Ley de Protección de Datos Personales de Andorra exige, para poder llevar a cabo una TID, que el país de destino cuente con una protección equivalente a la que contempla la normativa andorrana[4], salvo las excepciones previstas en la Ley[5] (más información en tabla anexa). Se entiende que tienen un nivel de protección equivalente los países miembros de la Unión Europea, y aquellos declarados como tal por la Comisión de la Unión Europea y/o por la Agencia Andorrana de Protección de Datos[6]
3. Comunicación a la Autoridad: No se requiere ni en el supuesto de que el país de destino cuente con protección equivalente a la exigida por la legislación nacional, ni cuando, en virtud de alguna de las excepciones previstas, se puedan transferir los datos personales a un país sin nivel de protección equivalente.
4. Autorización previa de la Autoridad: Tampoco se contempla la necesidad de obtener la previa autorización por parte de la autoridad competente para poder llevar a cabo una TID. No obstante la APDA sí tiene prevista, entre sus funciones, la de atender las consultas relativas a la validez de las TID a países que tienen una legislación que no ofrece el mencionado nivel de protección[7].

Argentina

Requisitos:

1. Consentimiento del titular: Se aplican las reglas previstas en la normativa argentina para la recogida y tratamiento de los datos personales. Se permiten las TID a un destino que no ofrece nivel de protección adecuado si el titular de los datos ha dado su consentimiento expreso al efecto[8].
2. Nivel de protección equivalente/adecuado en el destino: La legislación argentina prohíbe, con carácter general, las TID hacia países u organismos internacionales o supranacionales que no ofrezcan «niveles de protección adecuados»[9], si bien se prevén algunas excepciones (ver tabla comparativa anexa).

---

3 Llei 15/2003, del 18 de desembre, qualificada de protecció de dades personals, art. 3.14.
4 Idem, art. 35.
5 Idem, art. 37.
6 Idem, art. 36.
7 Decret del 9-06-2010 d'aprovació del Reglament de l'Agència Andorrana de Protecció de Dades, art. 25.9.
8 Decreto 1558/2001 de Reglamentación de la Ley n.º 25.326, art. 12.
9 Ley n.º 25.326, de Protección de los Datos Personales, art. 12.

3. Comunicación a la Autoridad: La legislación argentina vigente no condiciona las TID a la previa comunicación de las mismas a la Dirección Nacional de Protección de Datos Personales (DNPDP).
4. Autorización previa de la Autoridad: Tampoco se precisa actualmente la autorización previa de la DNPDP para las TID.

Chile

La normativa chilena define, de forma genérica, que la comunicación o transmisión de datos consiste en «dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.»[10]

Requisitos:

No se regulan de forma específica las TID, siéndoles de aplicación, básicamente, las mismas reglas que operan para la recogida y el tratamiento de datos personales.

1. Consentimiento del titular: Se aplican las reglas previstas en la normativa chilena para la recogida y tratamiento de los datos personales.
2. Nivel de protección equivalente/adecuado en el destino: No se exige en la normativa chilena vigente que el país de destino cuente con un nivel de protección equiparable al previsto en ella.
3. Comunicación a la Autoridad: No se exige actualmente por la legislación chilena que se deba comunicar las TID a la autoridad competente.
4. Autorización previa de la Autoridad: Tampoco es necesaria para las TID ningún tipo de autorización previa por autoridad judicial o administrativa alguna.

Colombia

Reglamentariamente, se establece que «la transferencia de datos tiene lugar cuando el Responsable y/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.»[11]

Adicionalmente, se prevé la figura de la «transmisión de datos», definida como el «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.»[12]

Requisitos:

1. Consentimiento del titular: Se aplican las reglas previstas en la legislación colombiana para la recogida y tratamiento de los datos personales. Se permiten las TID a un destino que no ofrece nivel de protección adecuado si el titular de los datos ha dado su autorización expresa e inequívoca al efecto[13].

---

10 Ley 19628 sobre protección de la vida privada, art. 2.ºc).

11 Decreto 1377 por el que se reglamenta parcialmente la Ley Estatutaria 1581 sobre disposiciones generales para la protección de datos personales, art. 3.4.

12 Idem, art. 3.5.

13 Ley Estatutaria N.º 1581, por la que se dictan disposiciones generales para la protección de datos personales, art. 26. a).

2. Nivel de protección equivalente/adecuado en el destino: Sí se exige que el país de destino cuente con un nivel de protección adecuado, que no podrá ser inferior al que exige la Ley colombiana[14].
3. Comunicación a la Autoridad: La legislación colombiana no exige actualmente la previa comunicación a la Superintendencia de Industria y Comercio (SIC).
4. Autorización previa de la Autoridad: No se prevé de forma expresa en la normativa colombiana vigente el requisito de la autorización previa por parte de la Autoridad competente. No obstante, para aquellos casos en que el país de destino no garantiza un nivel adecuado de protección, corresponde a la SIC emitir la declaración de conformidad relativa a la TID[15].

Costa Rica

Reglamentariamente, se establece que una transferencia de datos personales consiste en la «acción mediante la cual se trasladan datos personales, a un responsable de Datos Personales o un tercero»[16], sin que existan disposiciones vigentes adicionales relacionadas con el carácter internacional de la transferencia.

Requisitos:

1. Consentimiento del titular: Como regla general, se exige la autorización expresa y válida del titular para cualquier tipo de transferencia sea internacional o no.[17]
2. Nivel de protección equivalente/adecuado en el destino: No se exige este requisito actualmente por la normativa costarricense.
3. Comunicación a la Autoridad: Actualmente la legislación costarricense no exige la comunicación previa a la Agencia de Protección de Datos de los Habitantes (PRODHAB).
4. Autorización previa de la Autoridad: Tampoco exige la actual normativa de Costa Rica obtener la autorización previa de la PRODHAB.
5. Otros: Se requiere la existencia de un contrato entre el responsable de la transferencia de datos y el responsable receptor de los mismos, en el que se contemplen para éste, al menos, las mismas obligaciones que le son aplicables a aquél.[18]

España

La normativa española define a la TID como el «tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.»[19]

---

14 Idem, art. 26.
15 Idem, art. 26 parágrafo 1.
16 Decreto Ejecutivo N.º 37554-JP, Reglamento a la Ley de protección de la persona frente al tratamiento de sus datos personales, art. 2. w).
17 Ley n.º 8968 de Protección de la persona frente al tratamiento de sus datos personales, art. 14.
18 Decreto Ejecutivo N.º 37554-JP, Reglamento a la Ley de protección de la persona frente al tratamiento de sus datos personales, art 43.
19 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, art. 5.1.s).

Cabe señalar que la LOPD y su Reglamento disponen de Títulos específicos que regulan las características y requisitos de este tipo de comunicaciones de datos: («Movimiento internacional de datos» y «Transferencias internacionales de datos», respectivamente).

Requisitos:

1. Consentimiento del titular: Se aplican las reglas previstas en la legislación española para la recogida y tratamiento de los datos personales, sin que exista una particularidad en cuanto a este requisito referido a las TID, salvo por el hecho de que no será necesario que el país de destino prevea un nivel de protección equiparable al de la legislación española, si el titular ha dado su consentimiento inequívoco a la transferencia prevista.
2. Nivel de protección equivalente/adecuado en el destino: Es requisito general exigido que el país de destino tenga un nivel de protección equiparable al de la ley española, en caso contrario deberá obtenerse la autorización previa del Director de la Agencia Española de Protección de Datos (AEPD)[20], salvo que se trate de algunos de los supuestos excepcionados en la ley[21].
3. Comunicación a la Autoridad: Para las TID la normativa española requiere en todo caso la notificación previa a la AEPD[22].
4. Autorización previa de la Autoridad: Asimismo es necesario obtener la autorización previa del Director de la AEPD para los casos en que el país de destino de una TID no garantice un nivel de protección equivalente.

México

En México, con independencia de su destino, se considera «transferencia» a «toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.»[23]

Reglamentariamente, se especifica que «la transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado»[24] y se prevén condiciones y requisitos específicos para las TID.[25]

Requisitos:

1. Consentimiento del titular: En su art. 36, la LFPD establece que «el tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos».[26]

   Por su parte, el Reglamento de la LFPD prevé que «toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular», salvo que la misma esté prevista en las excepciones enumeradas en el art. 37 de la LFPD.
2. Nivel de protección equivalente/adecuado en el destino: Actualmente, la legislación mexicana no exige que el país de destino de una TID cuente con un nivel de protección equivalente al que brinda la propia legislación mexicana.

---

20 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, art. 33.
21 Idem, art. 34.
22 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, art. 66.3.
23 Ley Federal de Protección de Datos Personales en Posesión de los Particulares, art. 3, XIX.
24 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, art. 67.
25 Idem, ver: Capítulo IV, Sección III.
26 Ley Federal de Protección de Datos Personales en Posesión de los Particulares, art. 36. Énfasis añadido.

3. Comunicación a la Autoridad: En ningún caso se requiere efectuar una comunicación previa al IFAI para poder llevar a cabo una TID, con independencia de su país de destino.
4. Autorización previa de la Autoridad: En México, tampoco es necesario contar con autorización del IFAI para poder llevar a cabo una TID. Reglamentariamente se establece que si los responsables «lo consideran necesario», podrán solicitar la opinión del IFAI para que éste analice si las TID que aquéllos realicen cumplen con lo dispuesto por LFPD y su Reglamento.[27]
5. Otros: La normativa mexicana también indica que la transferencia deberá ser informada mediante el aviso de privacidad que prima en esta legislación y que la misma deberá limitarse a la finalidad que la justifique.

Nicaragua

La legislación nicaragüense define la cesión o transferencia como «la trasmisión de los datos personales a una persona distinta de su titular»[28] y regula de forma indistinta las cesiones o transferencias tanto nacionales como internacionales, salvo por la exigencia expresa de unos niveles de seguridad y protección adecuados que impone sobre los países u organismos internacionales de destino en las TID.

Requisitos:

1. Consentimiento del titular: Con carácter general la normativa nicaragüense obliga a obtener el consentimiento previo del titular de los datos para cualquier cesión o transferencia, incluidas, por tanto, las TID. Quedan exceptuados los supuestos en que lo disponga una ley, la TID se realice entre instituciones del Estado en el ejercicio de sus atribuciones, existan razones de salud pública, interés social o seguridad nacional, o se hubiere aplicado un procedimiento de disociación de datos suficiente de manera que no pueda identificarse a una persona determinada[29].
2. Nivel de protección equivalente/adecuado en el destino: Aunque contempla algunos supuestos de excepción, la Ley nicaragüense vigente exige, con carácter general, que el país u organismo internacional de destino de una TID proporcionen niveles de seguridad y protección adecuados[30].
3. Comunicación a la Autoridad: La Ley de Protección de Datos Personales de Nicaragua exige que el responsable del fichero informe a la Dirección de Protección de Datos Personales (DIPRODAP) sobre cualquier cesión o transferencia realizada, incluyendo por tanto las TID. No se indica expresamente si esta comunicación ha de ser anterior necesariamente a efectuarse la TID, dada la redacción del apartado f) del art. 15 de la LPDP, «deberá informar a la Dirección de Protección de Datos Personales, la transferencia de datos realizada», cabe entender que puede comunicarse con posterioridad a la TID.
4. Autorización previa de la Autoridad: En ningún caso se exige para las cesiones o transferencias, tampoco las internacionales, la previa autorización de la DIPRODAP.
5. Otros: Además de lo ya indicado en los párrafos precedentes, la legislación nicaragüense prevé otros requisitos que deben contemplarse en cualquier cesión o transferencia, incluidas las TID: a) Los fines de la cesión o transferencia deben estar directamente

---

27 Ver art. 76 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
28 Ley N.º 787, de 21 de marzo de 2012, de Protección de Datos Personales, art. 3.c).
29 Idem, art. 13.
30 Idem, art. 14.

relacionados con el interés legítimo del cedente y del cesionario, b) debe informarse al titular sobre la finalidad de la cesión e identificar al cesionario, y c) en toda cesión o transferencia debe seguirse un procedimiento específico, con unas obligaciones determinadas para cedente (o responsable del fichero) y cesionario (o solicitante)[31].

Perú

En el Perú, se define como «transferencia de datos personales» a «toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.»[32]

De manera particular, la legislación peruana regula la figura del «flujo transfronterizo de datos personales», definido como la «transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectúo la transferencia ni el tratamiento que reciban.»[33]

Reglamentariamente, se especifica que «se denomina flujo transfronterizo de datos personales a la transferencia de datos personales fuera del territorio nacional».[34]

Requisitos:

1. Consentimiento del titular: Como regla general, «para el tratamiento de los datos personales debe mediar el consentimiento de su titular»[35]; dicho tratamiento incluye su «comunicación por transferencia».[36] Dicho consentimiento deberá ser «previo, informado, expreso e inequívoco», si el país destinatario de los datos no cuenta con un nivel de protección adecuado conforme a la ley peruana y, además, el emisor del flujo transfronterizo de datos personales no garantiza que el tratamiento de los datos se efectúe conforme a dicha legislación.
2. Nivel de protección equivalente/adecuado en el destino: El art. 15 de la Ley 29733 del Perú dispone que el titular (el responsable) y el encargado del banco de datos personales «deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la presente Ley»[37]. Inmediatamente después, el mismo artículo establece que si el país destinatario no cuenta con un nivel de protección adecuado, «el emisor del flujo transfronterizo de datos personales» será el responsable de garantizar que el tratamiento de los datos se efectúe conforme a lo dispuesto por la ley de referencia.
3. Comunicación Previa a la Autoridad: El art. 26 del Reglamento de la Ley 29733 dispone que «en todo caso», los flujos transfronterizos de datos personales se pondrán «en conocimiento» de la Dirección General de Protección de Datos Personales (DGPDP), «incluyendo la información que se requiere para la transferencia de datos personales y el registro de banco de datos.»[38]

---

31 Idem, art. 15.
32 Ley 29733 de Protección de Datos Personales, art. 2.16.
33 Idem, art. 2.8.
34 Reglamento de la Ley 29733 de Protección de Datos Personales, art. 18.
35 Ley 29733 de Protección de Datos Personales, art. 5.
36 Ver, Idem art. 2.17.
37 Idem, art. 15.
38 Reglamento de la Ley 29733 de Protección de Datos Personales, art. 26.

4. Autorización de la Autoridad: Ni legal ni reglamentariamente se contempla la necesidad de obtener la autorización previa de la DGPDP para que en el Perú pueda llevarse a cabo una TID. No obstante, el primer párrafo del art. 26 antes referido, prevé que «los titulares del banco de datos personales o responsables del tratamiento,[39] podrán solicitar la opinión de la [DGPDP] respecto a si el flujo transfronterizo de datos personales que realiza o realizará cumple con lo dispuesto por» la Ley 29733 y su Reglamento.

Portugal

No cuenta con una definición legal específica. No obstante, la Lei da protecçâo de dados pessoais (Ley de protección de datos personales) regula las TID en su Capítulo III, a lo largo del cual, si bien no se menciona el término «internacional» o «internacionales», se hace referencia en todo momento a la circulación o transferencias de datos personales, entre estados, y en ningún caso a cesiones o transferencias en las que tanto emisor como destinatario se encuentran en Portugal.

Requisitos:

1. Consentimiento del titular: Se aplican las reglas contempladas en la legislación portuguesa relativas a la recogida y tratamiento de los datos personales. La única particularidad sobre el consentimiento del titular en cuanto a las TID, radica en que si el país de destino no goza de un nivel adecuado de protección, la Comisión Nacional de Protección de Datos (CNPD) puede permitir la TID si el titular presta de forma inequívoca su consentimiento para dicha TID.
2. Nivel de protección equivalente/adecuado en el destino: La Ley portuguesa no exige este requisito si el país de destino de la TID es miembro de la Unión Europea[40]. En caso contrario, la TID sólo podrá realizarse si el estado al que se transfieren los datos personales asegura un nivel de protección adecuado[41]. No se permite la transferencia a un estado sobre el que la Unión Europea haya considerado que no goza de protección adecuada. Asimismo, la normativa portuguesa recoge, en el art. 20 de la LPDP, una serie de excepciones a este requisito.
3. Comunicación a la Autoridad: La normativa portuguesa vigente no precisa que las TID deban ser comunicadas previamente a la CNPD.
4. Autorización previa de la Autoridad: Para aquellos supuestos en los que el país de destino no asegure un nivel adecuado de protección y no concurran ninguna de las excepciones que permiten la TID, será precisa la autorización de la CNPD, que podrá concederla cuando el responsable del tratamiento asegure mecanismos adecuados para garantizar la protección de la vida privada y los derechos y libertades fundamentales de los titulares de los datos.

República Dominicana

Expresamente, se dispone que una TID es un «tratamiento de datos que supone una transmisión de los mismos fuera del territorio de la República Dominicana, sin importar el

---

39 Cabe recordar que el artículo 2.14 del Reglamento de la Ley 29733 de Protección de Datos Personales define al «responsable del tratamiento» como «aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.»

40 Lei n.º 67/98, de 26 de Outubro, da protecçâo de dados pessoais, art. 18.

41 Idem, art. 19.

soporte, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del archivo de datos personales establecido en territorio dominicano.»[42]

Requisitos:

1. Consentimiento del titular: Resulta de aplicación la regla general que previene que «el tratamiento y la cesión de datos personales es ilícito cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias.»[43]
2. Nivel de protección equivalente/adecuado en el destino: La normativa dominicana vigente no exige que el país de destino proporcione a los datos personales un nivel de protección equivalente al que ésta proporciona.
3. Comunicación a la Autoridad: No se exige comunicación de las TID a la autoridad competente.
4. Autorización previa de la Autoridad: La normativa vigente tampoco exige autorización previa para realizar TID.
5. Otros: De conformidad al artículo 5.3.a) de la Ley Orgánica 172-13, deberá proporcionarse información al titular respecto de quiénes pueden ser destinatarios de sus datos personales o, en su caso, la clase de destinatarios. Por su parte, el artículo 80 del mismo ordenamiento dispone de forma taxativa los casos en que podrá llevarse a cabo «la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que requieran del consentimiento del titular de los datos».

Uruguay

Requisitos:

1. Consentimiento del titular: La Ley n.º 18.331 prevé que será posible realizar la transferencia internacional de datos cuando el interesado «haya dado su consentimiento inequívocamente a la transferencia prevista.»[44]
2. Nivel de protección equivalente/adecuado en el destino: Como regla general, «se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia»[45], con las excepciones previstas en la misma norma.
3. Comunicación a la Autoridad: Por vía de inscripción registral, los responsables deben comunicar la Unidad Reguladora y de Control de Datos Personales (URCDP) el destino de los datos y las personas físicas o jurídicas a las que pueden ser transmitidos, con independencia de su ubicación.[46]
4. Autorización previa de la Autoridad: La URCDP «podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías

---

42 Ley Orgánica 172-13 sobre protección de datos de carácter personal, art. 6.20
43 Idem, art. 5.4.
44 Ley n.º 18.331 de Protección de Datos Personales y Acción *Habeas Data*, art. 23.A).
45 Idem, art. 23.
46 Idem, art. 29.F).

suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos.»[47]

7.1.2 PAÍSES CON LEGISLACIÓN EN MATERIA DE *HABEAS DATA*

Bolivia, Ecuador, El Salvador, Honduras, Panamá y Paraguay, si bien carecen actualmente de una legislación específica sobre la materia, regulan ciertos aspectos sobre protección de datos personales y de *Habeas Data* a través de sus respectivas constituciones, así como de normas sectoriales.

En lo que a las TID se refiere, podemos decir que ninguno de estos de países cuenta actualmente disposiciones expresas que las regulen y que, en aquellos supuestos en que se trata una transmisión de información personal, exceptuando el caso de El Salvador, no se hace distinción en función de si el destino se encuentra o no en el extranjero.

Bolivia

Reglamentariamente[48] se establece que el tratamiento técnico de datos personales en el sector público y privado en todas sus modalidades, incluyéndose las transferencias, precisa el conocimiento y el consentimiento previos del titular, que será dado por escrito o medio equiparable en función de las circunstancias.

Los datos personales objeto de tratamiento sólo podrán ser transferidos a un tercero, previo dicho consentimiento del titular o en virtud de orden judicial.

Brasil

La, recientemente entrada en vigor, Lei 12.965 de 23 de abril de 2014, que regula el Marco Civil de Internet, aborda tangencialmente algunas cuestiones aplicables a las transferencias de datos personales, en las que debe entenderse incluidas las internacionales, por parte de los prestadores de servicios de la sociedad de la información. Así, para poder facilitar a terceros los datos personales de los usuarios, incluidos los registros de conexión y acceso a aplicaciones de Internet, se precisa, con carácter general, el consentimiento libre, expreso e informado del titular[49].

Actualmente el Proyecto de Ley de Protección de Datos Personales, contempla en su art. 35 la necesidad, con carácter general, de que el país de destino proporcione un nivel de protección equiparable y prevé otros supuestos en los que excepcionalmente podrán llevarse a cabo las TID.

El Salvador

Su Ley de Acceso a la Información Pública[50] dispone que los entes obligados a la misma deben adoptar las medidas que protejan la seguridad de los datos personales y eviten, entre otras cosas, su transmisión no autorizada, y no podrán difundir, distribuir o comercializar los

---

47 Ibid, in fine.

48 Decreto Supremo n.º 1793, de 13 de noviembre de 2013, Reglamento de la Ley n.º 164 General de Telecomunicaciones, art. 56.

49 Lei 12.965 de 23 de abril de 2014, Marco Civil de Internt, art. 7.VII.

50 Decreto n.º 534, de 30 de marzo de 2011, Ley de Acceso a la Información Pública.

datos personales a no ser que cuenten con el consentimiento expreso y libre, por escrito o por un medio equivalente, de los individuos a que haga referencia la información.

Por su parte, el Reglamento General de la Ley Penitenciaria[51] establece, respecto a los datos personales de los internos en centros penitenciarios, que las TID podrán efectuarse cuando exista cooperación o auxilio policial, judicial, o penitenciario conforme a los tratados o convenios suscritos, excepto los datos sensibles relativos a opiniones políticas, convicciones religiosas, filosóficas sobre su salud, que sólo podrán transmitirse previo consentimiento por escrito del interno, salvo que por razones de interés general lo disponga alguna ley.

Finalmente, la Ley de regulación de los Servicios de Información sobre el Historial de Crédito de las Personas[52], requiere, con carácter general, que las transferencias de los datos de crédito de los consumidores o clientes entre las agencias de información de datos y los agentes económicos cuenten con el consentimiento expreso y por escrito de los consumidores o clientes.

Ecuador

La Ley ecuatoriana n.º 67 de Comercio Electrónico, Firmas y Mensajes de Datos, en su art. 9 hace referencia a la protección de datos en relación con los mensajes de datos, y concretamente sobre transferencias (internacionales o no) indica que se requiere el consentimiento expreso del titular.

Honduras

El art. 27 de la Ley de Transparencia y Acceso a la Información Pública dispone que incurre en infracción administrativa quien, fuera de los casos legalmente previstos, transmita (entre otras conductas) datos personales contenidos en cualquier archivo, registro o base de datos de las Instituciones sujetas a esta Ley.

Panamá

El art. 24.4 de la Ley n.º 24 del 22 de mayo de 2002 que regula el servicio de información sobre el historial de crédito, exige el consentimiento expreso de los consumidores o clientes para la transmisión de su historial de crédito entre los agentes económicos y las agencias de información de datos.

Por su parte, la Ley n.º 3 del 5 de enero de 2000 General sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida, prohíbe que, sin el consentimiento del afectado o sin justa causa, se facilite información, se haga referencia pública o privada o se comunique acerca de la condición de la persona infectada.

Paraguay

Con carácter general, la Ley n.º 1682 que reglamenta la información de carácter privado, en su precepto 4.º prohíbe «dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables».

---

51 Decreto Ejecutivo N.º 95, de 14 de noviembre de 2000, Reglamento General de la Ley Penitenciaria.

52 Decreto Legislativo n.º 695, de 27 de julio de 2011. Ley de regulación de los Servicios de Información sobre el Historial de Crédito de las Personas, art. 14.d).

7.1.3 OTROS PAÍSES

Cuba

En Cuba no existe una ley o norma de diferente rango que regule de forma sistemática la protección de los datos personales.

En la Constitución de la República de Cuba no se contempla el derecho a la protección de los datos personales, ni se prevé de forma expresa el derecho o protección a la intimidad o a la privacidad de los individuos.

Guatemala

Actualmente, en la República de Guatemala no existe normativa que de manera específica regule las TID.

Puerto Rico

De lo dispuesto por la Ley n.º 111 de 7 de septiembre de 2005 de Información al Ciudadano sobre la Seguridad de Bancos de Información y la Ley n.º 39 de 24 de enero de 2012 de Notificación de Política de Privacidad, no es posible inferir una regulación general ni específica relativa a las TID.

En todo caso, la segunda de estas disposiciones, dirigida hacia los «operadores de páginas» de Internet, establece que será obligación de éstos notificar a sus usuarios sobre su Política de Privacidad, que entre otra información deberá contener «cualquier persona o entidad con los cuales el operador privado comparte la información personal recopilada y/o conservada»[53].

A tales efectos, la Ley de Notificación de Política de Privacidad no distingue sobre la ubicación de la persona o entidad con la que el «operador de páginas» de Internet puede llegar a compartir información personal, por lo que debe entenderse que la obligación de informar a los usuarios comprende la compartición de información fuera del territorio del Estado Libre Asociado de Puerto Rico.

Venezuela

Fuera del ámbito de la Constitución de la República Bolivariana de Venezuela, que en su artículo 28 expresamente contempla el derecho que toda persona tiene para conocer sobre el uso y finalidad de la información y de los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, a día de hoy Venezuela sigue sin contar con una ley que regule la protección de datos personales.

Se conoce que el Proyecto de Ley de Protección de Datos y *Habeas Data* de Venezuela contempla, en su artículo 51, que estará prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados. Al respecto, cabe destacar que el mismo proyecto de Ley no prevé, como excepción a esta obligación genérica, que el titular de los datos haya otorgado su consentimiento para la transferencia de sus datos.

---

[53] Ley n.º 39 de 24 de enero de 2012 de Notificación de Política de Privacidad, art. 3.1.b).

8. RELACIONES CON CANADÁ Y ESTADOS UNIDOS

8.1 CANADÁ

Canadá ha considerado tan importantes sus relaciones con la Unión Europea, y por ello con España y Portugal, que no sólo es que haya desarrollado legislación Estatal en materia de protección de datos personales, sino que se ha preocupado de obtener el reconocimiento de la Unión Europea de tener un «adecuado nivel de protección» mediante la Decisión de la Comisión 2002/2/CE de 20 de diciembre de 2001, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act* [notificada con el número C(2001) 4539][1]. E inclusive, en la actualidad el Estado de Quebec está intentando que se le reconozca este «nivel adecuado de protección[2]».

Por otro lado al ser parte del Tratado de libre comercio de América del Norte, tiene unas estrechas relaciones con México. Todo ello justifica unas pinceladas sobre su sistema normativo en protección de datos.

Canadá tiene un sistema co-regulatorio, como Australia, se trata de una variante del modelo comprensivo. Canadá cuenta con 27 leyes federales, provinciales y territoriales que regulan la protección de datos en el ámbito privado, público y de sanidad. A parte de estas normativas, también podemos encontrar la protección de datos en legislación anti-spam, relacionada con el robo de identidad o en el Código Penal.

En Canadá las autoridades encargadas de supervisar y garantizar la aplicación de estas leyes son los comisarios *(Information Privacy Commissioners* o *Ombudsmen)* a nivel federal, provincial y territorial.

«The Personal Information Protection and electronic documents Act», del 1998 es la ley a nivel federal dedicada a la protección de los datos y es de aplicación a la información recopilada, utilizada y comunicada por parte de el Gobierno federal, pequeño comercio, sector industrial y otras organizaciones siendo su finalidad promover la confianza en el comercio electrónico y transacciones del sector privado en Canadá, estableciendo unas mismas reglas de mercado para todas las empresas.

The Office of Information Privacy Commissioner of Canada (en Ottawa, Ontario) dispone de poderes para llevar a cabo auditorías e investigaciones a entidades que recopilan datos de ciudadanos canadienses, pueden recabar pruebas y documentos, realizar recomendaciones y conclusiones y elevar los casos a los tribunales cuando detecten algún incumplimiento. En alguna normativa sectorial se pueden incluso imponer sanciones. Por tanto, si bien tiene amplios poderes de supervisión, a diferencia del modelo europeo no dispone de los mismos mecanismos de ejecución o imposición de importantes sanciones.

Los individuos también pueden reclamar ante el Comisario de Canadá algún incumplimiento por parte de las empresas con el fin de que se lleve a cabo una investigación que puede acabar en los Tribunales. Los perjudicados igualmente pueden solicitar la correspondiente indemnización por los daños sufridos.

---

1 Diario Oficial n.º L 002 de 04/01/2002 p. 0013-0016.

2 Art. 29 WP Opinion 7/2014 on the protection of personal data in Quebec (EN) Adopted on 4 June 2014 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp219_en.pdf.

La normativa federal de Canadá permite la aprobación de normativas propias y similares en las diferentes provincias que contarán con una autoridad de protección de datos independiente. Estas normativas provinciales normalmente se aplicarán con carácter preferente a la normativa federal PIPEDA. Este caso se produce por ejemplo en las provincias de Alberta, British Columbia y Quebec.

Al igual que la normativa europea el consentimiento es una pieza clave para el tratamiento y cesión de los datos, así como la transparencia en la determinación de las finalidades, el concepto de calidad ligado a la limitación de datos recabados o de su utilización, cesión o retención, la aplicación de medidas de seguridad, el derecho de acceso y rectificación. Igualmente incorpora dos conceptos que, se han tenido en cuenta en la redacción del nuevo reglamento europeo y que deberían ser considerados en las normativas de los países sudamericanos: *«Accountability»* y *«Openness»* donde las organizaciones son responsables de los datos personales que controlan, deben facilitar información clara sobre sus prácticas y responder de su cumplimiento.

Las diferentes normativas de privacidad establecen provisiones destinas a garantizar la seguridad de los datos aunque generalmente no establecen requerimientos técnicos específicos.

En las normativas de Canadá si que hay algunas provisiones relativas a la notificación de violaciones de datos que nos recuerdan al sistema americano o el propuesto en el nuevo reglamento europeo.

En cuanto a las transferencias internacionales de datos, la entidad que comunica los datos sigue siendo responsable del cumplimiento de la normativa de privacidad y ha de adoptar las medidas oportunas para asegurar que el destinatario de estos datos, cumple las mimas previsiones.

En el caso de Alberta por ejemplo, se exige además que se informe en la política de privacidad sobre los países fuera de Canadá donde se tratarán los datos y las finalidades por las cuales se ha autorizado. Además, en el momento de la recogida o transferencia de los datos se ha de informar al individuo de qué modo podrá ejercer su derecho de acceso para obtener información sobre las políticas y prácticas de la organización en relación a sus proveedores fuera de Canadá y el nombre o cargo de la persona que podrá resolver cuestiones sobre el tratamiento de los datos por parte de los proveedores situados fuera de Canadá. Este último requerimiento también nos recuerda a la figura del DPO del nuevo reglamento europeo.

Desde Canadá también se han desarrollado los principios de *Privacy by Design and by Default* que, igualmente forman parte de la propuesta de reglamento europeo y que, también son deseables en cualquier normativa que se desarrolle en los países de América del Sur.

Sin duda el factor cultural es otra circunstancia importante que no hay que olvidar a la hora de elaborar leyes y garantizar su efectividad pues, si bien en algunos países las recomendaciones y códigos de conducta son una herramienta de gran valor en otros países, pueden no resultar tan efectivos si no van acompañados de un robusto sistema sancionador.

8.2 ESTADOS UNIDOS

Estados Unidos goza de una especial relación con diferentes Estados Iberoamericanos desde una cuádruple vertiente, de ahí la necesidad de tener una panorámica de un sistema normativo tan diferente a los estudiados con anterioridad.

Por un lado en lo que respecta a sus relaciones con la Unión Europea, y por ello con España y Portugal, que queda consagrado en el instrumento de *Safe Harbor,* que otorga a las empresas que se encuentren certificadas por este mecanismo, un nivel adecuado de protección a efectos

de transferencias internacionales. Aunque como veremos, este sistema se encuentra cuestionado en la actualidad tras las filtraciones del caso Snowden y no está garantizada su continuidad.

En una segunda y tercera ópticas tenemos por un lado a México que es parte del Tratado de libre Comercio de América del Norte (TLCAN) o North American Free Trade Agreement (NAFTA), del que además forman parte Estados Unidos y Canadá, y por otro lado Chile, que también ha firmado un Tratado de libre comercio con EEUU. Estos Tratados provocan flujos de datos y por ello transferencias internacionales de datos.

Como cuarta vertiente, se encuentra el caso de Puerto Rico, en calidad de Estado Libre Asociado y como último grupo tenemos a aquellos estados que debido a factores geoestratégicos, políticos, económicos o coyunturales, están mejorando sus relaciones con Estados Unidos.

En EEUU rige un sistema sectorial y de autorregulación en materia de privacidad y seguridad. Si bien algunos estados federales han reconocido el derecho a la privacidad en sus constituciones estatales (como California) y a través del *Common Law (Case Law)* se han reconocido ciertos derechos relacionados con la privacidad, con carácter general y en la Constitución Federal no existe propiamente un derecho fundamental a la protección de datos sino que, los datos de carácter personal se protegen a través de leyes que específicamente regulan un determinado sector de actividad (registros de crédito o bancarios, registros de alquiler de vídeos, ficheros de salud, etc.). Las leyes sectoriales, a menudo se utilizan como complemento de normativas más generales, con la finalidad de otorgar una protección específica a un determinado tipo de datos.

El sistema legislativo americano es bastante complejo por la cantidad de leyes y organismos encargados de su aprobación y ejecución. Existen las leyes federales, aprobadas por el Congreso que, son de aplicación general en todos los estados federales y que pueden o no, tener una aplicación preferente por encima de las estatales. Es decir que, muchas de estas leyes federales son desarrolladas con sus específicas características en muchos de los estados federales, como si de una directiva europea se tratara, obligando con ello a las empresas no solo a aplicar la ley federal sino también, cada una de las leyes estatales que les resulten de aplicación.

Por ejemplo, *«The US Telemarketing Sales Rules»* del año 1995 que ha sido modificada varias veces es una ley federal que no tiene aplicación preferente por encima de las al menos 42 leyes estatales aprobadas por los estados federales. Por tanto, para asesorar a una empresa sobre las llamadas que pueden realizar a los consumidores para la venta de productos y acciones de marketing hay que tener en cuenta no solo la citada ley federal sino también, las leyes estatales que le pueden ser de aplicación por ejemplo, si actúa en más de un estado federal.

Otras leyes, por ejemplo *«The Fair Credit Reporting Act»* (FCRA) aprobada el 1970 que, igualmente ha sido modificada varias veces es de aplicación preferente, y por tanto los estados federales no pueden regular o aprobar normativas que entren en conflicto con esta materia. A nivel EU sería parecido a un reglamento europeo, de aplicación obligatoria a todos los estados miembros.

Hay que tener en cuenta que, no solo el Congreso o los estados federales están facultados para aprobar leyes o normativas de desarrollo sino que, el Congreso puede delegar a las Agencias Federales (por ejemplo, a la Federal Trade Commission, a la Federal Communication Commission, etc.) la potestad de aprobar normativas adicionales. Por tanto, el marco normativo realmente es complejo y variado.

Repasando algunas de las normativas americanas más destacadas en cuestiones relacionadas con el tratamiento de datos y en el ámbito privado, encontraríamos:

La citada FCRA que limita el uso y finalidades de los informes de consumidores que compilan las agencias dedicadas a esta actividad (Consumer Reporting Agencies) y que, sirven como factor de elegibilidad de un usuario para poder optar a un trabajo, crédito, seguro,

negocio o ayudas gubernamentales. Esta ley establece mecanismos para garantizar la calidad y corrección de los datos, por ejemplo limitando el tipo de datos a recabar y permitiendo al usuario el acceso a estos informes y la posibilidad de discutirlos. También se establecen finalidades determinadas para poder utilizar estos datos y en algunos casos, es exigible el consentimiento previo del usuario.

«The Children's Online Privacy Protection Act» (COPPA) del año 2000, regula la recogida de datos de menores de 13 años a través de páginas web comerciales y establece una serie de requisitos para garantizar la información clara, el consentimiento previo por parte de los padres o tutores del menor y el derecho de oposición (opt-out), así como la confidencialidad, integridad y seguridad de los datos.

«Gramm-Leach-Bliley Act (GLBA)», esta norma federal reguladora del sector bancario y de los seguros incluyó en su capítulo V una serie de previsiones encaminadas a proteger la privacidad y seguridad de los datos tratados por este sector. Esta ley también cuenta con normativa complementaria para garantizar la seguridad de los datos (GLBA Safeguards Rule, 2003) que constan en soporte electrónico y papel. Esta ley federal a diferencia de la FCRA no tiene aplicación preferente por encima de las leyes estatales y por tanto, muchos estados han aprobado sus propias versiones incluyendo nuevos derechos y obligaciones.

«The Health Insurance Portability and Accountability Act (HIPPA)» del año 1996 y modificada varias veces, es la ley federal que regula los tratamientos y comunicaciones de datos de salud y resulta aplicable a determinadas entidades del sector de la salud (profesionales de la salud, planes médicos y otras entidades relacionadas). Esta ley está acompañada por una normativa específica dedicada a la seguridad de los datos en formato electrónico (HIPPA Security Rule, 2003) que establece la implantación de programas de seguridad, formación, evaluación de riesgos, etc. Al igual que GLBA, HIPPA no es de aplicación preferente y por tanto, hay que tener en cuenta la normativa estatal que pueda resultar de aplicación en cada caso.

«The Drivers Privacy Protection Act (DPPA)» del año 1994, también modificada posteriormente, protege la información personal de los conductores tratada por los departamentos estatales y oficinas de vehículos a motor. Esta norma tampoco goza de aplicación preferente y por tanto hay que ir estado por estado para determinar las finalidades, la posibilidad o prohibición de distribuir estos datos vía Internet, etc.

En el sector del marketing existen varias leyes federales que, sin disponer de aplicación preferente han sido desarrolladas por los diferentes estados federales. Por ejemplo, *«The US Telemarketing Sales Rules»* antes citada. Esta normativa establece ciertas reglas para realizar este tipo de llamadas en cuestiones de horario, llamadas automáticas, información clara, etc. En su modificación del año 2003 incluyó el *«Do-Not-Call Registry»* que es parecido al concepto de «lista Robinson» para evitar recibir llamadas de tele marketing. Algunos estados incluso han desarrollado su propio registro *Do-Not-Call* con lo que, la aplicación práctica para una empresa que actúa en varios estados es bastante compleja.

Otros ejemplos de este sector: *«Telephone Consumer Protection Act»* del 1991 y *«The Junk Fax Prevention Act»* del 2005 dedicadas a limitar los envíos de faxes con finalidades comerciales. Son normas federales que tampoco gozan de aplicación preferente por encima de las leyes aprobadas por los estados federales con lo que, los requisitos varían de estado a estado.

Y finalmente *«Controlling the Assult of Non-Solicited Pornography and Marketing Act»* del 2004 (CAN-SPAM Act), ley federal cuya finalidad es limitar el envío de correos comerciales por parte de cualquier anunciante que desee promocionar sus productos o servicios vía email desde o hacia EEUU. Se establecen mecanismos de *opt-out* (oposición), información transparente y reglas especiales para los servicios móviles. Una importante diferencia con el

sistema establecido a nivel de la UE con la Directiva 2002/58/CE de privacidad y comunicaciones electrónicas es que, no existe el concepto de *«existing business relationship»* en esta ley en concreto (aunque si existe en otras leyes americanas que hemos citado del sector del marketing) y por tanto, no se distingue entre destinatarios con los que previamente hemos tenido una relación comercial, de los que no.

Una de las normativas americanas que ha sido considerada en la propuesta de reglamento europeo consiste en la notificación de violaciones de datos. Normativa desarrollada a nivel estatal en cada estado federal. La primera de ellas fue la de California SB1386 *Security Breach Notification Rule* del año 2003. Después de esta, muchos estados federales han aprobado normativas parecidas en su ámbito de aplicación. A diferencia de los casos anteriores, en este campo no hay una ley federal, al menos de momento. Ello implica también la dificultad de aplicar esta normativa cuando el ámbito de actuación de la empresa se amplia a más de un estado.

En el sector público igualmente existen varias normas que afectan al tratamiento de los datos, por ejemplo, *«The Privacy Act»* del 1974 que establece una serie de requerimientos y garantías en el tratamiento y recogida de datos por parte de las agencias federales o gubernamentales. *«The Freedom of Information Act»* del 1966 que garantiza, con una serie de excepciones, el derecho de acceso de los ciudadanos a ciertos registros custodiados por las agencias federales.

Por otro lado, también existe otro grupo de normativa que, con la finalidad de cumplir sus objetivos establecen la obligación de facilitar información personal en determinados casos.

Quizás la más conocida, *«The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act» (USA PATRIOT Act)* del 2001 nacida a raíz de los actos terroristas del 11S para aumentar la seguridad nacional contra ataques de este tipo. Para cumplir estos objetivos se aumenta la cooperación y el intercambio de información entre las entidades financieras y gubernamentales con el fin de detectar actividades relacionadas con actividades terroristas o de blanqueo de capitales.

Con finalidades similares encontramos otras leyes como *«US Bank Secrecy Act»* o *«International Money Laundering Abatement and antiterrorist Financing Act»*.

En el ámbito de las telecomunicaciones *«The US Communications Assistance to Law Enforcement Act»* (CALEA) del 1994 establece una serie de requerimientos a las empresas de telecomunicaciones para cooperar en la interceptación de comunicaciones por ejemplo, cuando sea necesario por razones de seguridad o cumplimiento de una ley.

También hay otras leyes que obligan a las empresas a comunicar ciertos datos a las agencias federales o estatales por cuestiones de salud pública, seguridad, ocupación, etc. y evidentemente, cuando un Juzgado o tribunal requiere ciertos datos en interés de la justicia.

Las consecuencias derivadas del incumplimiento de las diferentes normativas, es diferente en cada caso, hay sanciones civiles y penales, incluyendo en algunos casos prisión, multas, resarcimiento de daños y perjuicios, etc

Los problemas a que se enfrenta el sistema americano consiste en que la legislación acostumbra a ir por detrás de los avances tecnológicos, circunstancia que se comparte con la normativa de la UE, igualmente no existe una única entidad o agencia que supervise las numerosas normativas que existen en materia de protección de datos, lo que a veces implica conflictos, superposición de leyes y complejidad a la hora de cumplir con las obligaciones. Por ejemplo, en la aplicación de las normas antes indicadas puede intervenir no solo la Federal Trade Commission sino, la Federal Communication Commission o Reguladores de las Instituciones Financieras estatales o federales (Office of Comptroller of Currency, Federal Reserve…), o del ámbito de la salud (US Department of Health and Human Services: Office of Civil Rights,…), US Treasury Department, a nivel estatal los fiscales generales («State Attorneys General»), etc.

Igualmente, algunas de estas normativas estatales o federales contemplan un derecho a favor de los individuos denominado «*private right of action*» que consiste en que, cualquier persona que ha sufrido un daño derivado de la violación de una ley tiene derecho a demandar al infractor y en algunos casos, permite reclamar indemnización por los daños. Por ejemplo, este derecho existe en la FCRA, GLBA SB1 de California, algunas *Security Breach Notification rules* (California, Nevada, New Hampshire, North Carolina, Tennessee, etc.), TCPA, DPPA, *The Privacy Act,* entre otras.

Uno de los mecanismos más destacados e importantes del sistema americano que serian deseables en las normativas europeas o en los países sudamericanos es la *Class Action* que permite a un grupo de personas en circunstancias similares demandar a otra parte, normalmente se trata de un grupo de consumidores que demanda a grandes negocios. A nivel europeo la figura más parecida, son las demandas que se permiten interponen, en ciertos casos, por parte de organizaciones de consumidores y usuarios. No obstante, no revisten la trascendencia y alcance de la *Class Action.*

El sistema americano también se caracteriza por su autorregulación que comparte con otros países como Japón o Singapur, deriva de la existencia de otros mecanismos que también contribuyen a la protección de los datos personales y que consisten en la aprobación de códigos de conducta y sellos de calidad a los que se someten las empresas y que son creados por entidades independientes, organismos industriales, grupos de empresas o por alguna empresa en particular (por ejemplo, BBBOnline, TRUSTe, Direct Marketing Association…).

Finalmente cabe destacar otra herramienta interesante de protección a los consumidores frente a prácticas comerciales engañosas o desleales, se trata de la Sección 5 de la Federal Trade Commission Act y recuerda a la normativa europea de consumidores y usuarios. Esta normativa protege a los consumidores de conductas comerciales engañosas, que incluyan manifestaciones falsas u omitan información relevante así como, las actuaciones desleales que causen daños sustanciales o pérdida de beneficios a los consumidores cuando no sea razonablemente posible de evitarlo. Una de sus aplicaciones prácticas más interesantes reside en toda la información que se facilita al usuario al recabar sus datos o en los avisos legales de las páginas web. El concepto de expectativa de privacidad es muy importante en estos casos para valorar si, con la información facilitada al usuario y atendiendo al caso concreto (dependiendo del sector de actividad, por ejemplo), era razonable esperar unas medidas de seguridad más estrictas o que los datos no se comunicaran a determinados terceros.

Por tanto, si bien en EEUU no tienen un sistema comprensivo como el modelo europeo y muchos países de América del Sur, si hay herramientas y mecanismos que son deseables y efectivos para mejorar la aplicación práctica. Algunos de ellos, incluso han sido considerados en la propuesta de nuevo reglamento europeo (sellos de calidad, códigos de conducta, normativa sectorial que tenga en cuenta las características de cada sector de actividad, notificación de las violaciones de datos). No obstante, sigue siendo deseable que los países europeos y de América del Sur adopten mecanismos para dotar al usuario de un poder más contundente para proteger sus derechos en el ámbito de la privacidad y en el mundo digital, uno de ellos podía ser la mencionada Class Action.

9. RELACIONES CON LA UNIÓN EUROPEA

A lo largo del presente Estudio hemos podido comprobar que existen claramente dos bloques de países iberoamericanos, aquellos que no cuentan con legislación sobre protección de datos y como mucho en sus textos constitucionales regulan la figura del *Habeas Data*, y aquellos que, o bien tienen Proyectos de Ley en tramitación parlamentaria, o ya cuentan con legislación en materia de protección de datos personales.

Es precisamente es este segundo bloque de países el que merece una especial atención, ya que las normativas existentes o en preparación, como se puede observar a lo largo del presente Estudio, se encuentran influenciadas por la Directiva 95/46/CE[1] y por el Convenio 108 del Consejo de Europa[2], por lo que o bien, sus normativas pueden nacer ya obsoletas o adolecen de las mismas deficiencias que la normativa comunitaria (y por ello las legislaciones española y portuguesa) a la hora de abordar los nuevos retos en privacidad surgidos de los avances tecnológicos como *Internet of Things, Big Data, smartphones* u otros dispositivos *wearables,* redes sociales, *cloud computing,* etc.

Las ventajas competitivas que podían tener con respecto al grupo de países que todavía no han regulado la materia pueden desaparecer, e inclusive los dos países que en la actualidad tienen reconocido por la Unión Europea el «nivel adecuado de protección[3]» a la hora de realizar transferencias internacionales podrían perderlo si no readaptan sus normativas a las nuevas figuras que salvaguardan la privacidad ante la revolución tecnológica que se está produciendo, o aquellos que se estuvieran planteando solicitarlo no lo obtuvieran.

No hay que perder de vista que a la hora de instalarse una multinacional en la zona, tener reconocido el nivel adecuado de protección puede ser un valor determinante a la hora de decidirse por un país u otro, de la misma manera que a la hora de contratar un servicio de *Cloud Computing* el saber que los servidores están ubicados en alguno de estos países puede también ser determinante para su elección.

Como acabamos de comentar, la Unión Europea ya hace tiempo que se dio cuenta que la Directiva 95/46/CE no contaba con mecanismos útiles y eficaces para los nuevos retos y desafíos en privacidad ante los avances tecnológicos reseñados. Ello llevó a la Comisión Europea a presentar el 25 de enero de 2012 su Propuesta de Reglamento del Parlamento europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general

---

1 Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

2 Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

3 Estos países son:
Argentina mediante Decisión de la Comisión de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (2003/490/CE). DOUE L 168/19 de 5.7.2003.
Uruguay: Decisión de Ejecución de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales [notificada con el número C(2012) 5704] (1) DOUE L 227/11 de 23.8.2012.

de protección de datos)[4], actualmente en trámite mediante procedimiento legislativo de Codecisión.

Tomando de base el texto aprobado en Primera Lectura por el Parlamento Europeo el 12 de marzo del 2014[5] y a la espera que el Consejo de la Unión Europea logre llevar a un acuerdo sobre la totalidad del la Propuesta de Reglamento (hasta el momento el acuerdo es sólo sobre capítulos concretos) que permita avanzar en la adopción de la misma, procederemos a destacar las principales novedades, principios y figuras que puede llegar a introducir y regular la más que probable futura normativa.

CUESTIONES GENERALES

EXCEPCIÓN BASADA EN EL TRATAMIENTO DE DATOS EN EL ÁMBITO PERSONAL O DOMÉSTICO (ART. 2)

La excepción basada en el tratamiento de datos en el ámbito personal o doméstico se matiza, indicando que, ésta excepción se aplicará asimismo a la publicación de datos personales cuando quepa esperar razonablemente que solo accederán a ella un número limitado de personas. Se introduce así una figura similar a la «expectativa de privacidad» existente en la legislación mexicana.

AMPLIACIÓN DEL ÁMBITO TERRITORIAL DE APLICACIÓN (ART. 3, 25)

Las empresas que tengan un establecimiento en un estado miembro deberán aplicar el reglamento aunque los tratamientos de datos se realicen fuera de la UE.

También se aplicará el reglamento a las entidades ubicadas fuera de la UE cuando su oferta de bienes y servicios se dirija a personas residentes en el territorio Europeo o las actividades de tratamiento permitan el control de estos interesados. Además, en estos casos, el responsable deberá designar un representante en la Unión, excepto algunos casos[6].

NUEVAS DEFINICIONES (ART. 4)

Entre las que destacan:

— Datos seudónimos.

— Elaboración de perfiles.

---

4 Propuesta de reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Bruselas 25.1.2012 COM (2012) 11 final. 2012/0011 (COD).

5 Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011-C7-0025/2012-2012/0011(COD)) (Procedimiento legislativo ordinario: primera lectura).

6 Cuando esté establecido en un tercer país considerado de protección adecuada, se traten datos de menos de 5000 interesados durante un período consecutivo de 12 meses y no se trate de datos de localización, sensibles, relativos a los niños o empleados, organismos públicos, o cuando se ofrezcan sus servicios de forma ocasional.

— Violación de datos personales.

— Datos genéticos.

— Datos biométricos.

— Datos relativos a la salud.

— Establecimiento principal.

— Representante.

— Empresa.

— Grupo de empresas.

— Normas Corporativas Vinculantes.

— Niño: toda persona menor de 18 años.

MECANISMOS DE DESARROLLO NORMATIVO (ART. 21, 85 TER)

La normativa prevé la existencia de mecanismos de desarrollo normativo que faciliten la aplicación práctica del reglamento. Concretamente, se encarga al Consejo Europeo de Protección de Datos (posteriormente explicaremos que es este Organismo) que dicte directrices, recomendaciones y mejores prácticas en relación a los diferentes apartados (por ejemplo, en la recogida de consentimiento a los menores, en el tratamiento de datos sensibles, etc.).

Igualmente los estados miembros o la legislación de la unión podrán limitar y desarrollar los diferentes apartados del reglamento.

Y se habilita a la Comisión para que, en función de las especiales características y sectores y situaciones de tratamiento de datos, para elaborar formularios normalizados, en los supuestos que se contemplan en el articulado.

NUEVAS CATEGORÍAS ESPECIALES DE DATOS (ART. 9)

El reglamento relaciona nuevas categorías especiales de datos incluyendo:

— Identidad de género,

— Datos genéticos y biométricos,

— Sentencias, sospechas de delito,

— Medidas de seguridad afines a condenas penales.

PRINCIPIOS GENERALES DE LA PROTECCIÓN DE DATOS (ART. 10 BIS)

Los principios generales de la Protección de Datos se mantienen pero se matizan y también se incluyen otros nuevos. Se establece el derecho a obtener una compensación por daños y perjuicios derivados de una operación de tratamiento ilícita.

Se reitera que estos derechos se ejercerán, en general, sin coste alguno.

Igualmente se indica de forma general que, el responsable del tratamiento de los datos responderá a las solicitudes de los interesados en un plazo razonable.

CONDICIONES PARA EL CONSENTIMIENTO (ART. 7)

Se refuerza la obligación del consentimiento, siendo necesario que se distinga claramente si se facilita en el contexto de otro asunto. Igualmente ha de ser tan fácil retirar el consentimiento como otorgarlo.

TRATAMIENTO DE DATOS PERSONALES DE MENORES (ART. 8)

Se dedica una especial atención al consentimiento otorgado por menores de edad con la finalidad de proteger sus intereses. El consentimiento de menores de 13 años solo será válido si ha sido dado o autorizado por sus padres o representantes legales.

Se establece una obligación por parte del responsable de hacer esfuerzos razonables para verificar tal consentimiento, considerando la tecnología disponible y sin generar un tratamiento innecesario de datos.

La información que se facilite será con un lenguaje claro adecuado al público destinatario.

DERECHO DE ACCESO (ART. 15)

El derecho de acceso se amplia incluyendo el derecho a obtener la siguiente información:

— Información relativa a la seguridad del tratamiento de los datos,

— Plazo durante el cuál se conservarán los datos o criterios para determinar este plazo,

— La intención de transferir datos a un tercer país u organización internacional,

— Información sobre la existencia de elaboración de perfiles, medidas y efectos para el interesado

— Información significativa sobre la lógica utilizada en los tratamientos automatizados.

— etc.

Este derecho también se vincula al concepto de portabilidad.

Si un interesado ha facilitado datos personales y estos se tratan por vía electrónica, tiene derecho a que el responsable le facilite copia de estos datos en un formato electrónico interoperable que le permita seguir utilizándolos.

Cuando sea técnicamente viable, se facilitará la transmisión de estos datos se realizará directamente entre el responsable y el proveedor seleccionado por el interesado.

DEBER DE INFORMACIÓN (ARTS. 13 BIS Y 14)

El deber de información se amplia, no solo deberá facilitarse la información prevista en el apartado anterior sino que, deberá combinarse con la utilización de iconos informativos normalizados.

Antes de recabar los datos del interesado, éste deberá tener acceso de forma previa a los iconos visuales que se indican a continuación y posteriormente se le facilitará la información previa indicada en punto anterior.

DERECHO DE RECTIFICACIÓN (ART. 16)

Se mantiene el derecho a obtener del responsable del tratamiento la rectificación de los datos personales cuando resulten inexactos o a que se completen cuando resulten incompletos mediante una declaración rectificativa adicional.

PRINCIPIO DE TRANSPARENCIA (ARTS. 10A, 11, 12, 13, 13 BIS)

El principio de transparencia está muy presente en toda la Propuesta del Reglamento, obliga al responsable a aplicar políticas concisas, transparentes, sencillas y fácilmente accesibles por lo que respecta al tratamiento de datos y ejercicio de derechos.

La información se ha de facilitar de forma inteligible, utilizando un lenguaje sencillo y claro, especialmente si se dirige a los niños. Cuando sea posible y se traten datos automatizados, se proporcionarán medios para que las solicitudes se hagan por vía electrónica.

Obligación de notificación en caso de rectificación y supresión a los destinatarios a quien se han transferido los datos (art. 13)

DERECHO DE OPOSICIÓN (ARTS. 19, 20)

El derecho de oposición se complementa con el derecho de oposición a la realización de perfiles. El interesado ha de ser informado de una forma claramente visible de la existencia de estos tratamientos.

La elaboración de perfiles que dé lugar a medidas que produzcan efectos jurídicos o afecten a los intereses y derechos del interesado, no se basarán únicamente en un tratamiento automatizado y deberán incluir una evaluación humana y una explicación de la decisión alcanzada tras dicha evaluación.

DERECHO A LA SUPRESIÓN (ART. 17)

El derecho de supresión se completa con una referencia al derecho al olvido[7], con la obligación de suprimir los datos y abstenerse de darles más difusión. El interesado también podrá obligar a los terceros a suprimir todos los enlaces a los datos, copias o reproducciones de los mismos en determinados casos[8].

Si la difusión de estos datos se ha realizado en vulneración del reglamento, el responsable deberá adoptar todas las medidas razonables para que los datos sean suprimidos, también por los terceros y el interesado tendrá derecho a reclamar del responsable o encargado del tratamiento una indemnización por el perjuicio sufrido.

NUEVAS OBLIGACIONES

RENDICIÓN DE CUENTAS DEL RESPONSABLE («*ACCOUNTABILITY*») (ART. 22)

El responsable deberá adoptar políticas e implementar medidas técnicas que puedan ser verificables y permitan demostrar la idoneidad y eficacia de las medidas en cumplimiento del Reglamento. Se establece la necesidad de establecer controles del cumplimiento y realizar auditorías cada 2 años.

PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO (ART. 23)

En el momento de determinación de los fines del tratamiento y los medios, el responsable implementará las mejores prácticas y medidas para el tratamiento de los datos conforme al reglamento, respetando los principios de privacidad y garantizando la protección de los derechos de los interesados.

Esta protección se tendrá en cuenta durante todo el ciclo de vida de los datos, desde su recogida hasta su tratamiento y supresión.

El responsable también garantizará que, por defecto, solo se traten datos personales que sean necesarios para cada finalidad específica y que no se conserven o divulguen más allá del mínimo necesario. Principio de minimización de datos y de su conservación.

CORRESPONSABLES DEL TRATAMIENTO (ART. 24)

Cuando se determinen conjuntamente los fines y medios del tratamiento por varios responsables estos pueden responder solidariamente del tratamiento si no han establecido previamente de forma clara cuales son las responsabilidades y obligaciones de cada parte.

---

7 Recientemente el Tribunal de Justicia de la Unión Europea del 13/05/2014 C-131/12 (Costeja y AEPD *vs*. Google) también se ha pronunciado a favor del «derecho al olvido» y actualmente, se está trabajando para analizar y valorar su aplicación práctica, circunstancia que podrá afectar al texto que se apruebe definitivamente.

8 Cuando los datos ya no son necesarios para los fines para los que se recogieron, cuando se retira el consentimiento o se ejercita el derecho de oposición, cuando los datos han sido tratados ilícitamente o un tribunal o autoridad de la UE obliga a la supresión de los datos.

ENCARGADO DEL TRATAMIENTO (ARTS. 26, 27)

Se mantiene la figura del encargado del tratamiento y se obliga a que su relación con el responsable se regule por un contrato escrito entre ambas partes que determine las obligaciones de cada parte, estableciendo que el encargado del tratamiento permitirá inspecciones *in situ*.

Tanto el encargado de tratamiento como las personas que actúen bajo la autoridad del encargado o responsable del tratamiento, estarán sometidos a las instrucciones que reciban del responsable del tratamiento, salvo que esté obligado a hacerlo por disposición normativa del derecho de la Unión Europea o de algún Estado miembro.

DOCUMENTACIÓN (ART. 28)

Debe elaborarse documentación en materia de seguridad que permita demostrar el cumplimiento de los requisitos del reglamento, informando del nombre y datos del contacto del responsable o del delegado de protección de datos (si lo hubiera).

RELACIÓN CON EL RIESGO (ART. 32 BIS)

Tanto el responsable como el encargado del tratamiento (si es el caso) deberán llevar a cabo un análisis de riesgos de los efectos potenciales del tratamiento de datos previsto sobre los derechos y las libertades de los interesados, y valorar si es probable que las operaciones de tratamiento presenten riesgos específicos.

Se entiende que es probable que presenten riesgos específicos:

— Tratamiento de datos personales de más de 5 000 interesados durante un periodo consecutivo de 12 meses,

— El tratamiento de categorías especiales de datos personales datos de localización o datos relativos a niños o empleados en ficheros a gran escala,

— La elaboración de perfiles en base a los cuales se adopten medidas que produzcan efectos jurídicos que afecten significativamente a la persona,

— El tratamiento de datos personales para la prestación de atención sanitaria, investigaciones epidemiológicas o estudios relativos a enfermedades mentales o infecciosas, cuando los datos sean tratados con el fin de tomar medidas o decisiones sobre personas concretas a gran escala,

— El seguimiento automatizado de zonas de acceso público a gran escala

— Otras operaciones de tratamiento para las cuales sea necesaria la consulta del delegado de protección de datos o de la autoridad de control

— Una violación de los datos personales que probablemente afecte de forma negativa a la protección de los datos personales, la privacidad, los derechos o los intereses legítimos del interesado,

— Las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados,

— La facilitación de datos personales a un gran número de personas que no cabe esperar razonablemente que sea limitado.

El análisis de riesgos se revisará a más tardar un año después, o inmediatamente si la naturaleza, el alcance o los fines de las operaciones de tratamiento de datos cambian significativamente

EVALUACIÓN DE IMPACTO (ARTS. 30, 33, 33 BIS)

En relación a las medidas de seguridad, se establece la necesidad de adoptar medidas adecuadas tomando en consideración el resultado de la realización de una evaluación de impacto relativa a la protección de datos. Esta será obligatoria en los supuestos que hemos visto anteriormente que son probables que entrañen riesgos específicos.

La evaluación deberá tener en cuenta la gestión de los datos personales durante todo el ciclo de vida, desde la recogida y el tratamiento hasta la supresión. Su contenido y alcance mínimo queda delimitado en el mismo reglamento que también obliga a establecer revisiones periódicas, al menos cada 2 años.

NOTIFICACIÓN DE UNA VIOLACIÓN DE DATOS A LA AUTORIDAD DE CONTROL O INTERESADOS (ARTS. 31, 32, 32 BIS)

Se establece la obligación de notificación a la autoridad de control de las violaciones de datos, sin demora injustificada, incluyendo al menos la naturaleza de la violación de datos, categorías, número de interesados, ID del delegado PD, recomendaciones.

Debe quedar documentado y permitir a la autoridad de control verificarlo.

La autoridad de control mantendrá un registro público de los tipos de violaciones notificadas.

Después de la notificación a la autoridad de control, se notificará al interesado sin demora injustificada, cuando sea probable que la violación de datos afecte negativamente a la protección de los datos personales, con un lenguaje claro y sencillo. La autoridad de control, considerando los efectos negativos probables podrá exigir al responsable que haga la notificación al interesado, si no lo ha hecho antes.

CONSULTAS PREVIAS (ART. 34)

Se establece la obligación de consultar al delegado de protección de datos o a la autoridad de control antes de proceder al tratamiento de datos en determinados casos en que el tratamiento entrañe un nivel de riesgo elevado.

DELEGADO DE PROTECCIÓN DE DATOS (ARTS. 35, 36, 37)

La figura del delegado de protección de datos es obligatoria en determinados tratamientos:

— Tratamiento de datos a más de 5000 interesados durante un periodo consecutivo de 12 meses.

— De categorías especiales de datos.

— De datos de localización.

— De monitorización del interesado.

— De menores.

— De empleados a gran escala.

— Administraciones públicas.

El DPO ha de ser el punto de enlace entre la Autoridad de control y el responsable o encargado del tratamiento aunque, la responsabilidad del tratamiento sigue residiendo en el responsable.

HERRAMIENTAS PARA FACILITAR EL CUMPLIMIENTO

CÓDIGOS DE CONDUCTA (ART. 38)

Se promueve la creación de códigos de conducta elaborados por las autoridades de control para contribuir a la correcta aplicación del reglamento y teniendo en cuenta las características de los distintos sectores de tratamiento de datos.

CERTIFICACIÓN (ART. 39)

Se prevé la creación de un sello Europeo de Protección de Datos para contribuir a la confianza y transparencia en el tratamiento de los datos, reforzando el principio de *Accountability*.

El sello es voluntario y asequible, y certifica tratamientos concretos, no empresas en todos sus tratamientos.

Estos sellos serán facilitados por las autoridades de control una vez superado un proceso de certificación realizado por profesionales acreditados y tendrá una duración máxima de 5 años.

Se establecerá un registro público donde el público podrá ver los certificados válidos e inválidos expedidos en el estado miembro.

La obtención de un sello podrá evitar una posible sanción económica.

TRANSFERENCIAS INTERNACIONALES DE DATOS

La principal novedad es que, a nivel Europeo el instrumento que regulará esta disciplina es un Reglamento EU que será directamente aplicable a cada estado miembro de la Unión, sin necesidad de transposición. Este sistema permitirá homogenizar las normativas de los estados miembros y garantizar una efectiva libre circulación de datos desde el territorio de la Unión hacia el exterior.

Así mismo, permitirá un importante ahorro de costes a las empresas que actúan en más de un estado miembro. Igualmente, a nivel internacional los mecanismos existentes para las transferencias internacionales de datos se mejoran (especialmente el esquema basado en las normas corporativas vinculantes y procedimientos de autorización previa) y amplían incluyendo nuevos mecanismos, como el sello europeo de protección de datos.

PRINCIPIOS GENERALES, NIVEL ADECUADO DE PROTECCIÓN, GARANTÍAS APROPIADAS (ARTS. 41, 42, 43, 44)

Para que las transferencias internacionales que realizan los responsables y encargados de tratamiento sean legitimas, deberán cumplir uno de los siguientes supuestos:

Podrá realizarse una transferencia cuando la Comisión haya decidido que el tercer país, o un territorio o un sector de tratamiento de datos en ese tercer país, o la organización internacional de que se trate garantizan un «nivel de protección adecuado de protección».

Cuando no disponemos de este nivel adecuado de protección se pueden realizar transferencias internacionales a un tercer país o una organización internacional:

Siempre que ofrezcan garantías adecuadas, por ejemplo:

— Normas corporativas vinculantes *(Binding Corporate Rules):* Se pueden realizar transferencias internacionales de datos entre empresas de un mismo grupo que dispongan de normas corporativas vinculantes. El reglamento facilita la adopción de este mecanismo que facilita a las empresas globales a realizar transferencias internacionales de datos entre sus filiales en cumplimiento de la normativa europea.
— Se disponga de un «Sello Europeo de Protección de Datos» válido para el responsable y el destinatario.
— Mediante cláusulas tipo de protección de datos adoptadas por una autoridad de control y con validez general,
— En estos 3 casos anteriores, no será necesaria autorización previa de la autoridad de control.
— Mediante cláusulas tipo de protección de datos que requieran autorización previa de una autoridad de control. En este caso, cuando el tratamiento de datos afecte a varios estados miembros, la legitimidad de las transferencias se puede facilitar mediante un mecanismo de coherencia que consiste en la cooperación de las distintas autoridades de control para facilitar el proceso.

Cuando sea de aplicación alguna de las excepciones previstas: por ejemplo, cuando contamos con el consentimiento del afectado para realizar la misma, o en desarrollo o ejecución de un contrato en el que el interesado sea parte o se celebre o ejecute «en su interés».

PETICIONES DE REVELACIÓN DE DATOS PERSONALES (ART. 43 BIS)

Si una resolución de un juzgado o tribunal o de una autoridad administrativa de un tercer estado requiere a un responsable o encargado de tratamiento para que rebele o haga públicos datos personales deberá comunicarlo sin demora injustificada a la autoridad de control que deberá estudiar el caso y decidir si lo autoriza.

COOPERACIÓN INTERNACIONAL (ARTS. 45, 45 BIS)

Las autoridades de control y la Comisión quedan facultadas para tomar las medidas apropiadas con terceros países y organizaciones internacionales destinadas a crear mecanismos que garanticen la aplicación de las legislaciones de protección de datos y la asistencia administrativa mutua, consulta sobre conflictos jurisdiccionales, entre otros. Muy útil esta disposición debido a los fenómenos de la globalización y geodeslocalización que provoca Internet.

AUTORIDADES NACIONALES DE CONTROL

CREACIÓN (ARTS. 46, 47, 53, 54)

Se fomenta una mayor coordinación y cooperación entre las diferentes autoridades de control, siendo muy importante la homogenización de sus poderes públicos que hasta ahora

eran diversos en cada estado miembro (amplios poderes de inspección e investigación, imposición de importantes sanciones, suspender flujos de datos o prohibir tratamientos, otorgar certificaciones, etc.).

Todo ello sin duda, va a contribuir en una aplicación coherente y uniforme del presente Reglamento en toda la Unión. Igualmente se insiste en la independencia e imparcialidad que las autoridades deben garantizar en el ejercicio de las funciones.

COMPOSICIÓN Y DEBER DE SECRETO (ARTS. 48, 49, 50)

Los estados miembros establecerán los mecanismos y requisitos del nombramiento, renuncia y cese de los miembros de la autoridad de control, de acuerdo con una serie de parámetros y principios.

Sus miembros estarán obligados durante el mandato, así como a la finalización del mismo a guardar secreto profesional sobre las informaciones confidenciales que hayan conocido en el ejercicio de sus funciones.

COMPETENCIAS, FUNCIONES Y PODERES (ARTS. 51, 52, 53, 84)

Cada autoridad de control actúa en su propio estado miembro salvo cuando se aplica un mecanismo de coherencia o cuando un interesado ejercita su derecho a presentar reclamación o recurso ante una autoridad de control. Cuando se trata de entidades públicas sus tratamientos solo pueden controlarse por la autoridad de ese Estado.

Destaca la posibilidad de actuar conjuntamente con otras autoridades de control y prestar asistencia mutua, lo que amplia el ámbito territorial de actuación de las autoridades de control fuera de sus fronteras. También cabe destacar la posibilidad de establecer una tasa ante la presentación de solicitudes que se puedan llegar a entender como «manifiestamente excesivas».

En lo que respecta a los poderes de las autoridades de control, se delimitan de una manera más clara y como se ha indicado, se amplían en su tipología (prohibir temporal o definitivamente los tratamientos, suspender flujos de datos a terceros países, ordenar la rectificación o supresión de datos, conceder certificaciones,…).

INFORME DE ACTIVIDAD (ART. 54)

Las autoridades de control elaborarán un informe de actividad, al menos, cada dos años, el cuál pondrán también a disposición del público en general.

AUTORIDAD DE CONTROL PRINCIPAL Y ASISTENCIA MUTUA (ARTS. 54 BIS, 55)

Es sin duda una de las mayores novedades de la propuesta de reforma y quizá la que mayor debate y recelos despierta en el proceso legislativo.

Se trata del principio conocido como *«one stop shop»:* Cuando un responsable esté establecido en más de un estado miembro o trate datos de residentes de varios estados miembros, la autoridad de control donde esté establecido el establecimiento principal actuará como principal autoridad de control de las actividades de tratamiento de responsable en todos los estados miembros.

La autoridad principal deberá utilizar un procedimiento de consulta a las demás autoridades de control y tras ello adoptar las medidas oportunas. Si se producen conflictos de competencia,

el Consejo Europeo de Protección de Datos emitirá un dictamen e incluso podrá decidir sobre la asignación de la autoridad competente.

OPERACIONES CONJUNTAS (ART. 56)

Con el fin de facilitar la coordinación entre las autoridades de control, se contempla la posibilidad de que puedan llevarse a cabo tareas conjuntas de investigación, medidas represivas u otras operaciones en las que participen miembros designados o personal de las autoridades de control de otros Estados miembros. Cuando nos encontremos en el supuesto de una actuación llevada a cabo por una autoridad principal de control, las de los otros Estados implicados tendrán derecho a participar en la misma.

COHERENCIA

MEDIDAS DE COHERENCIA, DICTAMEN DEL CONSEJO EUROPEO DE PROTECCIÓN DE DATOS, ACTOS DE EJECUCIÓN, MEDIDAS DE URGENCIA, EJECUCIÓN (ARTS. 57, 58, 58 BIS, 60 BIS, 61, 62, 63)

Con el fin de garantizar la coherencia en la aplicación e interpretación del Reglamento, se establece que, antes de aplicar determinadas medidas destinadas a producir efectos jurídicos amplios, las autoridades de control comunicará el proyecto de medida al Consejo Europeo de Protección de Datos, y a la Comisión, quienes podrán solicitar que cualquier asunto de aplicación general, sea tratado en el marco del mecanismo de coherencia que; mecanismo también aplicable a los casos individuales.

En el mecanismo de coherencia la autoridad principal de control comunica al resto de autoridades de control afectadas la propuesta de resolución, pudiendo paralizarla si realizan «objeciones graves».

Cualquier medida de ejecución dictada por una autoridad de control será ejecutable en toda la Unión Europea. Carecerán de validez jurídica y por ello, no serán ejecutables las medidas dictadas por la autoridad de control cuando siendo preceptivo, no se sometan al mecanismo de coherencia o se dicten existiendo «objeciones graves».

CONSEJO EUROPEO DE PROTECCIÓN DE DATOS

CREACIÓN, COMPETENCIAS, COMPOSICIÓN, CONFIDENCIALIDAD E INDEPENDENCIA (ARTS. 64, 65, 66, 67, 68, 69, 70, 71, 72)

El Consejo Europeo de Protección de Datos sustituirá al actual Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, más conocido por su denominación en inglés art 29 WP. Se adaptan sus funciones y competencias a las nuevas figuras creadas por la propuesta de Reglamento, consolidándose como el órgano de coordinación de las autoridades de control de los Estados miembros.

RECURSOS, RESPONSABILIDAD Y SANCIONES

RECLAMACIONES Y RECURSOS (ARTS. 73, 74, 75, 76, 77)

Cualquier interesado que considere que el tratamiento de sus datos personales no se ajusta a la normativa vigente tiene derecho a presentar una reclamación ante la autoridad de control

de cualquier Estado miembro. Igualmente podrán presentarlas las organizaciones, organismos y asociaciones que representen un interés público.

Producida la decisión de la autoridad de control sobre ese asunto, el interesado tendrá derecho a interponer un recurso judicial contra esa decisión o inclusive, si la decisión de la autoridad de control es la de un Estado en el que el individuo no tiene su residencia habitual, tiene derecho a que la autoridad de control de su residencia habitual ejercite en su nombre una reclamación contra esa resolución.

Igualmente toda persona que haya sufrido un perjuicio, incluidos los daños no pecuniarios, como consecuencia de una operación de tratamiento ilícito o de un acto incompatible con el Reglamento tendrá derecho a reclamar del responsable o encargado del tratamiento una indemnización por el perjuicio sufrido.

Esta reclamación podrá ejercitarse alternativamente o bien en el Estado donde el responsable o encargado tiene algún establecimiento o bien en el Estado donde el reclamante tiene su residencia habitual, salvo que la reclamación judicial se dirija a una autoridad pública de la Unión o de un Estado miembro en ejercicio de sus poderes.

SANCIONES (ARTS. 78, 79)

Se trata de otro de los puntos que mayor debate ha generado, debido a la elevación de la cuantía de las sanciones. Se pretende armonizar la imposición de sanciones en el territorio de la Unión.

Además de la imposición de sanción pecuniaria (hasta 100.000.000 € o el 5 % de su volumen de negocios anual a escala mundial en el caso de una empresa, si esta última cifra fuera mayor), se puede imponer una advertencia escrita si es un primer incumplimiento no deliberado o, la realización de auditorías periódicas de protección de datos.

A la hora de graduar las sanciones se tendrán en cuenta factores como la gravedad, duración, negligencia o intencionalidad, la reiteración, el nivel de perjuicio, la categoría de datos, la colaboración con la autoridad de control, la privacidad por diseño, tener nombrado delegado en protección de datos, seguridad del tratamiento, evaluación de impacto, revisiones periódicas, etc.

CATEGORÍAS ESPECIALES DE TRATAMIENTO

TRATAMIENTO DE DATOS PERSONALES Y LIBERTAD DE EXPRESIÓN (ART. 80)

Se prevé que, para determinados artículos del Reglamento, los Estados miembros puedan establecer exenciones o excepciones tendentes a conciliar la protección de datos personales con la libertad de expresión. Estas disposiciones legislativas deben ser comunicadas sin demora la Comisión.

ACCESO A DOCUMENTOS PÚBLICOS (ART. 80 BIS)

Esta medida trata de conciliar la protección de datos personales con el acceso de los ciudadanos a los documentos públicos, más comúnmente conocido como «transparencia», quedando habilitadas las comunicaciones de documentos públicos cuando sea conforme a la legislación de la Unión o del Estado miembro.

DATOS DE SALUD (ART. 81)

Se establece que, el tratamiento de datos de salud sólo puede traer causa del derecho de la Unión o del Estado miembro, regulando algunos tratamientos específicos como la medicina preventiva, del trabajo, diagnóstico médico, asistencia sanitaria, interés público y salud pública, seguros de salud, etc, quedando habilitados estos tratamientos si los efectúan profesionales sanitarios con deber de secreto profesional o personas con obligación análoga de confidencialidad, según el supuesto concreto.

TRATAMIENTO DE DATOS EN EL ÁMBITO LABORAL (ART. 82)

Los Estados miembros quedan autorizados para emitir normas que regulen tratamientos de datos personales en determinadas materias de las relaciones laborales. Se prohíben la elaboración de perfiles y la utilización de datos con fines secundarios.

El consentimiento del empleado no constituye una base habilitante para el tratamiento si este no se ha obtenido libremente.

Se prohíben los tratamientos de datos no conocidos, pero se permite a los Estados legislar para aquellos supuestos en los que sea necesario investigar ante la sospecha que el empleado ha cometido un delito o grave incumplimiento en su actividad laboral, debiendo estar contemplados los plazos adecuados para la supresión de los mismos.

Se establecen reglas especiales para la videovigilancia prohibiéndose la oculta, control de los medios informáticos y realización de reconocimientos médicos.

SEGURIDAD SOCIAL (ART. 82BIS)

Siempre y cuando existan razones de interés público, los Estados miembros podrán dictar normas específicas para el tratamiento de datos personales relacionados con la seguridad social por parte de las administraciones públicas que, igualmente deberán ser comunicadas a la Comisión.

TRATAMIENTOS PARA FINES HISTÓRICOS, ESTADÍSTICOS O CIENTÍFICOS (ART. 83)

Para que puedan tratarse datos personales con fines de investigación histórica, estadística o científica deberá ser necesario que no sea posible cumplir con estas finalidades utilizado otros tratamientos, que no permitan la identificación de los interesados, o incluya mecanismos para evitar la reidentificación.

TRATAMIENTO DE DATOS PERSONALES POR SERVICIOS DE ARCHIVOS (ART. 83 BIS)

Los tratamientos de datos por parte de los servicios de archivos de las administraciones públicas, a la hora de permitir el acceso y consulta de estos documentos, deberán respetar la normativa de cada Estado miembro, en base a las normas establecidas en el Reglamento.

NORMAS VIGENTES SOBRE PROTECCIÓN DE DATOS DE LAS IGLESIAS Y ASOCIACIONES RELIGIOSAS (ART. 85)

En el momento de la entrada en vigor del Reglamento las normas que apliquen las iglesias, asociaciones o comunidades religiosas para la protección de datos personales serán válidas siempre que no contradigan a lo previsto en el Reglamento.

10. CONCLUSIONES

Comentábamos con anterioridad, en concreto en capítulo relativo a relaciones con la Unión Europea, que existen claramente dos bloques de países iberoamericanos, aquellos que no cuentan con legislación sobre protección de datos y como mucho en sus textos constitucionales regulan la figura del *Habeas Data,* y aquellos que, o bien tienen Proyectos de Ley en tramitación parlamentaria, o ya cuentan con legislación en materia de protección de datos personales.

Este segundo bloque de países cuenta con normativas vigentes o en preparación muy influenciadas por la Directiva 95/46/CE y por el Convenio 108 del Consejo de Europa, con el fin último de lograr que la Comisión Europea por medio de Decisión reconozca un nivel adecuado de protección. Recuérdese que Argentina y Uruguay lo tienen reconocido y que Uruguay a ratificado el Convenio 108, lo que permitiría a priori afirmar que cuentan con una ventaja competitiva sobre otros países de la región, puesto que al facilitarse las transferencias internacionales de datos (y con ello agilizándose los plazos y reduciéndose los costes y la burocracia), la instalación de una filial de una multinacional en un país u otro de la región, o la contratación un servicio de *Cloud Computing* dependiendo del lugar de alojamiento del servidor puede decantar la balanza aun lado o al otro.

Pero esto no es así desde el momento en el que la Unión Europea constata que la Directiva 95/46/CE y otra normativa aplicable, no cuentan con mecanismos suficientes y adecuados para afrontar los nuevos retos, oportunidades y amenazas en privacidad que suponen los avances tecnológicos como el *Big Data,* el denominado Internet de las Cosas, el *Cloud Computing,* el aumento de las app, la geodeslocalización, los robos masivos de datos, las brechas de seguridad, los fenómenos virales en redes sociales o aplicaciones de mensajería instantánea o los nuevos tipos delictuales surgen del uso de las nuevas tecnologías como la suplantación o robo de identidad digital, el *sexting,* la *sextortion,* el *ciberbullying* o el *grooming*.

No es sólo que la Unión Europea esté tratando de aprobar su Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), sino que mientras que esto se produce, está adaptando la normativa existente a las nuevas necesidades, retos y tendencias en materia de protección de datos de carácter personal, sino que hay un proceso de adaptación paralelo al trámite legislativo.

A un conocedor de la materia no se le puede escapar la gran labor de adaptación a estos nuevos escenarios con las Directivas 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, o Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), que esta realizando el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, más conocido como Art. *29 Working Party.*

A través de sus dictámenes, declaraciones, informes anuales o notas de prensa[1], están elaborando una doctrina que ayuda a la resolución de casos y problemas existentes, prepara la llegada de las nuevas herramientas y mecanismos de protección en privacidad, difumina la posibilidad de quiebra entre el modelo jurídico existente y el que está por llegar dando visos de

---

[1] http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm.

continuidad y consolida la coordinación de las Autoridades Nacionales de Control de cara a su reforzamiento en el futuro[2].

Resulta evidente que, si bien muchos son los países que ya cuentan con normativa específica en materia de protección de datos, nos encontramos con otros países iberoamericanos que deberían o bien iniciar procesos legislativos que culminen con normativas de nueva generación, o bien readaptar sus normativas a los nuevos tiempos como ya lo están haciendo, recientemente Chile y México actualizando sus normativas, o países como Honduras que se encuentran tramitan sus proyectos de ley.

Sólo con normativas de protección de datos flexibles antes los diferentes tipos de tratamientos de datos personales, que impliquen al empresario, entidad o administración pública durante todo el ciclo de vida del dato incluyendo conceptos como el *privacy by design* o *accountability,* que dispongan de herramientas innovadoras y eficaces a los nuevos tipos de tratamiento como puede ser la realización previa de un PIA *(Privacy Impact Assessments)*, que sean capaces de adaptar el cumplimiento de la normativa vigente a sus características (como adaptar la política de privacidad y el deber de información a un dispositivo de pantalla reducida), que permitan la implantación de soluciones imaginativas e innovadoras como la forma de obtención de consentimientos inequívocos en dispositivos variopintos (de pantalla normal o reducida, *wearables* o fijos, que por la amplitud del colectivo pueda existir una brecha digital, o no, etc), que ante el riesgo por perdida o fuga de datos permitan adoptar las medidas de seguridad y respaldo más adecuadas al volumen, tipología y sistema de tratamiento de datos (servidor físico, servidor virtual en modalidad de *Cloud Computing,* etc) y que conciban la protección de datos como una ventaja competitiva hacia el cliente que aportan un valor añadido y una imagen de calidad al producto o servicio promoviendo la creación de Sellos y Códigos de Conducta certificables sujetos a renovación periódica. En definitiva entendemos que las nuevas legislaciones deben incluir entre sus principios inspiradores la transparencia, la rendición de cuentas o *accountability* y la mejora continua.

Tampoco debemos olvidar que por los fenómenos de la geodeslocalización y transnacionalidad intrínsecos a las nuevas tecnologías, las diferentes legislaciones deben igualmente delimitar meticulosamente el ámbito territorial y material de aplicación y contar con mecanismos que permitan la unificación legislativa y la coordinación y cooperación con otros Estados y Organizaciones Supranacionales que eviten la impunidad de determinadas conductas, actividades o comisión de delitos amparándose en Estados sin regulación en la materia, que bien podrían denominarse paraísos cibernéticos.

También adquiere notable importancia el apartado educativo y de concienciación tanto de los que manejan datos como de los que los suministran. No se trata sólo de fomentar la cultura de la privacidad, concienciando a los ciudadanos sobre las cautelas que deben tener antes de facilitar sus datos personales e inculcar a responsables y encargados de tratamientos principios de transparencia, calidad de los datos, minimización de los datos, inocuidad para el afectado, rendición de cuentas, implantación de medidas técnicas y organizativas y controles y revisiones periódicas a las mismas, sino que hay que educar y formar en el uso de esas tecnologías que impidan que se ahonde la denominada brecha entre nativos y no nativos digitales.

Especial atención debería prestarse a la formación e información dirigida a los progenitores o responsables legales de menores, que les advierta de los riesgos que el uso de las nuevas tecnologías puede provocar en menores, para que así puedan educarlos, formarlos y

---

[2] En este sentido y a título ejemplificativo y no exhaustivo, en el link de la nota anterior en idioma inglés se pueden encontrar documentos sobre *right to be forgotten, Big Data, Internet of Things, security breaches, accountability, smart metering, geolocation services on smart mobile devices, Cloud Computing, personal data breach notification, apps on smart devices, privacy impact assessments, risk-based approach*.

concienciarlos. Sólo desde esa óptica se puede proteger al menor sin invadir su derecho al libre desarrollo de la personalidad y su intimidad. No se trata por tanto de controlar sus accesos, restringirlos o prohibirlos aunque sea tecnológicamente posible.

En otro orden de cosas debemos señalar que no todas las conductas contra la intimidad y privacidad de las personas son merecedoras de sanción administrativa, sino que debido a su gravedad deben requerir la interposición de una sanción penal. Los Ciberataques que provocan fugas masivas de datos tanto en administraciones públicas como en empresas o entidades privadas, la agravación de las consecuencias de determinados tipos penales por el fenómeno viral y de las redes sociales y sistemas de mensajería instantánea con una mayor número de posibles destinatarios, la aparición de nuevos tipos delictuales que utilizan las nuevas tecnologías para ampararse en el anonimato, y los robos o suplantaciones de identidad digital requieren soluciones novedosas e innovadoras y sobre todos herramientas y mecanismos de unificación legislativa, cooperación y coordinación de los Estados a nivel internacional que impidan que estos delincuentes se alojen ellos o alojen sus servidores y herramientas en países sin legislación o con escasa regulación en la materia.

En definitiva, como bien señala la Declaración de México D.F. del Observatorio Iberoamericano de Protección de Datos «Hacia la implantación de garantías para la protección de datos en los tratamientos de *Big Data*[3]» los datos personales son el oro de la economía digital, lo que se denomina monetización de los datos, al considerarse un activo y tener por ello un valor económico. Pero no todo lo tecnológicamente posible debe ser humanamente aceptable. Se trata de utilizar las ventajas que aportan las nuevas tecnologías y sus usos y no de demonizarlas regulando su uso mediante unos principios básicos de transparencia, seguridad, calidad de los datos, inocuidad para el afectado, minimización y rendición de cuentas que concilien estos dos extremos. Alcanzar esta conciliación requerirá, como ya hemos comentado, regular donde no se ha hecho y modificar donde sí se hizo. Como todo en la vida, no es positiva la «tecnofobia» ni la «tecnofascinación» pero si la tecnoreflexión y sobre todo la ética en los tratamientos de datos personales.

---

[3] Fue presentada el sábado 23 de agosto de 2014, en el transcurso de la Jornada académica de protección de datos personales en Internet, dentro de la bienvenida para los alumnos de la cuarta generación de la Maestría en Derecho de las Tecnologías de la Información y Comunicación de INFOTEC, en la ciudad de México Distrito Federal. Disponible en:
www.oiprodat.com/declaracion-de-mexico-d-f/.

TABLAS Y ANEXOS

CONSTITUCIONES NACIONALES

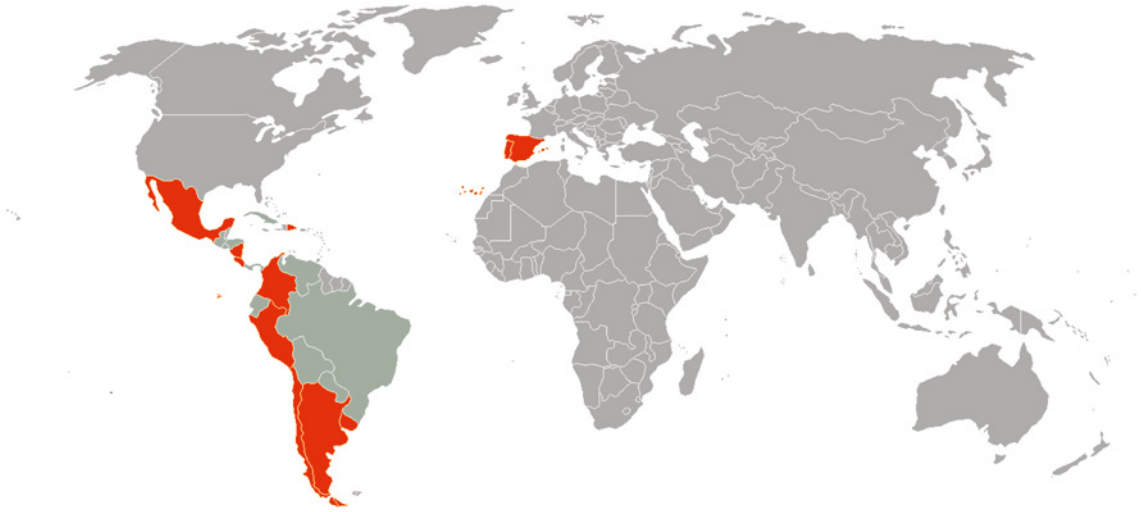
	Artículo	Texto
Andorra	Artículo 14	Se garantiza el derecho a la intimidad, al honor y a la propia imagen. Toda persona tiene derecho a ser protegida por las leyes contra las intromisiones ilegítimas en su vida privada y familiar.
Argentina	Artículo 43	Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.
Bolivia	Artículo 21	Las bolivianas y los bolivianos tienen los siguientes derechos: 2. A la privacidad, intimidad, honra, propia imagen y dignidad.
Brasil	Artículo 5	LXXII se concederá «habeas data»: a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo (…) LXXVII son gratuitas las acciones de «habeas corpus» y «habeas data» y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía.
Chile	Artículo 19	La constitución asegura a todas las personas: 4.º El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.
Colombia	Artículo 15	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 los 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.

	Artículo	Texto
Costa Rica	Artículo 23	El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley.
Ecuador	Artículo 66.19	El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.
El Salvador	Artículo 2	Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
España	Artículo 18.4	La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
Guatemala	Artículo 24	Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.
Honduras	Artículo 76	Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen.
México	Artículo 6	La información sobre la vida privada y los datos personales en los archivos gubernamentales serán protegidos conforme a las leyes secundarias.
Nicaragua	Artículo 26	Toda persona tiene derecho: A su vida privada y la de su familia; A la Inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo (…). A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información
Panamá	Artículo 29	La correspondencia y demás documentos privados son inviolables y no pueden ser ocupados o examinados sino por disposición de autoridad competente, para fines específicos y mediante formalidades legales. (…) se guardará reserva sobre los asuntos ajenos al objeto de la ocupación o del examen. Igualmente, las comunicaciones telefónicas privadas son inviolables y no podrán ser interceptadas (…).

	Artículo	Texto
Paraguay	Artículo 135	Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.
Perú	Artículo 2	Toda persona tiene derecho a: 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal (…). Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.
Portugal	Artículo 35	1. Derechos de los ciudadanos. 2. La ley define el concepto de datos personales, y las condiciones aplicables a su tratamiento automatizado, conexión, transmisión y utilización, y garantiza su protección por medio de un órgano administrativo independiente. 3. Límites utilización de la informática. 4. Prohibición Acceso a los datos personales de terceros, salvo en casos excepcionales previstos por la ley. 5. Prohibida la atribución de un número nacional único a los ciudadanos. 6. Acceso libre general garantizado a las redes informáticas para uso público, definiendo la ley el régimen aplicable a los flujos transfronterizos de datos y las formas apropiadas de protección de datos personales. 7. Protección datos personales mantenidos en ficheros manuales.
República Dominicana	Artículo 44.2	Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos.
Uruguay	Artículo 7	Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad.

	Artículo	Texto
Venezuela	Artículo 28	Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados (…) conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas (…).

LEGISLACIONES NACIONALES PROTECCIÓN DE DATOS



	Norma	Reglamento
Andorra	Llei 15/2003, de 18 de diciembre, qualificada de protecció de dades personals.	Decret de l'1-7-2004 d'aprovació del Reglament del registre públic d'inscripció de fitxers de dades personals.
Argentina	Ley 25.326 de protección de datos del 2 noviembre de 2000.	Decreto 1558/2001, por el que reglamenta la Ley de protección de datos.
Chile	Ley 19.628 sobre protección de datos de carácter personal.	Decreto 779/2000, por el que se reglamenta la Ley 19.629, que regula el registro de bancos de datos personales a cargo de los organismos públicos.
Colombia	Ley Estatutaria 1581, de 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.	Decreto 1377, de 27 de junio de 2013, por el cual se reglamenta parcialmente la Ley N.º 1581.
Costa Rica	Ley n.º 8968 de protección de la persona frente al tratamiento de sus datos personales.	Decreto Ejecutivo n.º 37554-JP, del 30 de octubre de 2012, por el que se reglamenta la Ley n.º 8968.
España	Ley Orgánica 15/1999 del 13 de diciembre de protección de datos de carácter personal.	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

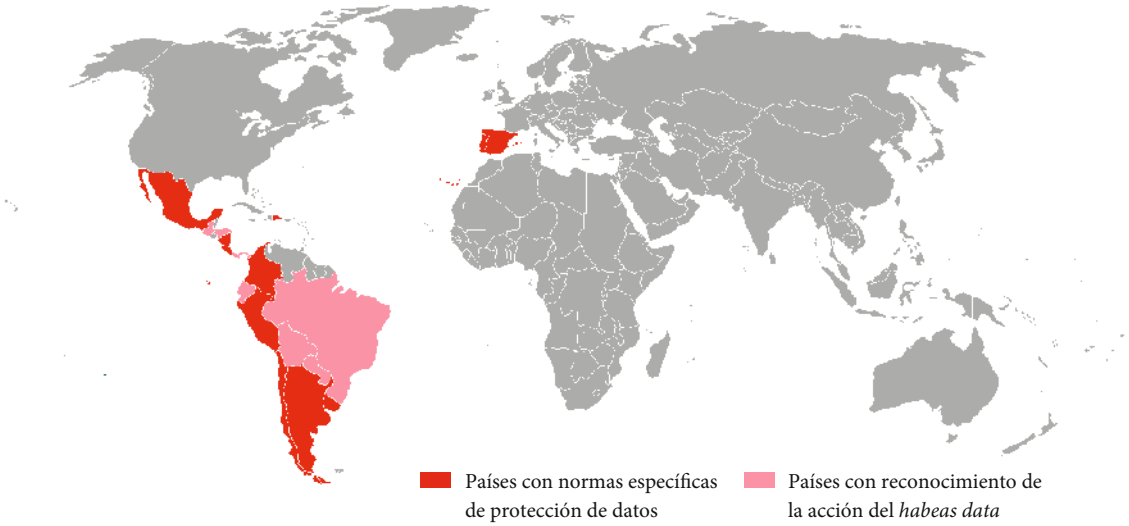
	Norma	Reglamento
México	Ley Federal de protección de datos personales en posesión de particulares.	Reglamento de la Ley Federal de protección de datos personales en posesión de los particulares.
Nicaragua	Ley n.º 787 de protección de datos personales.	
Perú	Ley n.º 29733, de 3 de julio de 2011, de protección de datos personales.	Decreto Supremo n.º 003-2013-JUS, de 21 de marzo de 2013, por el que se aprueba el Reglamento de la Ley n.º 29733.
Portugal	Lei 67/98, de 26 de Outubro de protecção de dados pessoais.	
Puerto Rico	Ley n.º 39 de 24 de enero de 2012 de notificación de política de privacidad.	
República Dominicana	Ley Orgánica 172-13 de protección de datos de carácter personal de la República Dominicana.	
Uruguay	Ley n.º 18.331 de 11 de noviembre de 2008, de protección de datos personales y acción habeas data.	Decreto n.º 664/008, de 22 de diciembre de 2008 por el que se crea el registro de bases de datos personales, adscrito la Unidad Reguladora y de Control de Datos Personales. Decreto n.º 414/009, de 31 agosto de 2009, por el que se reglamenta la Ley de protección de datos personales y el habeas data.

LEGISLACIÓN ESPECÍFICA COMPARADA

	Andorra	Argentina	Chile	Colombia	Costa Rica	España
Deber de información	X	X		X	X	X
Niveles de seguridad	Discrecional	X		X	X	X
Derechos ARCO	X	X	X	X	X	X
Documento de seguridad	Discrecional	X		X	X	X
Medidas de seguridad	X	X		X	X	X
Inscripción de ficheros	X	X	X	X	X	X
Autoridad de control	X	X	X	X	X	X
Sistema de sanciones	X	X	X	X	X	X

	México	Nicaragua	Perú	Portugal	Rep. Dominicana	Uruguay
Deber de información	X	X	X	X	X	X
Niveles de seguridad		X	X	X	Datos sensibles	
Derechos ARCO	X	X	X	X	X	X
Documento de seguridad	X		X			
Medidas de seguridad	X	X	X	X	X	X
Inscripción de ficheros		X	X	X	X	X
Autoridad de control	X	X	X	X	Prevista, no creada	X
Sistema de sanciones	X	X	X	X	X	X

NIVELES DE PROTECCIÓN CONFORME A LA NORMATIVA PROPIA DE CADA PAÍS



Países con normativa específica de protección de datos	Países con reconocimiento de la acción del *habeas data*	Países con normativa en materia de privacidad	Países sin normativa sobre protección de datos
Andorra	Bolivia	Paraguay	Cuba
Argentina	Brasil	Puerto Rico	El Salvador
Chile	Ecuador		Venezuela
Colombia	Guatemala		
Costa Rica	Honduras		
España	Panamá		
México			
Nicaragua			
Perú			
Portugal			
República Dominicana			
Uruguay			

PAÍSES CON NIVEL ADECUADO DE PROTECCIÓN

	Decisión de la Comisión
Andorra	Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010
Argentina	Decisión de la Comisión de 30 de junio de 2003
Uruguay	Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012

PAÍSES ESPECIALMENTE RELACIONADOS

	Decisión de la Comisión
Canadá	Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001
Estados Unidos	Acuerdo de Puerto Seguro con los Estados Unidos de América. Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

PROYECTOS LEGISLATIVOS EN TRÁMITE

	Proyecto normativo	Año
Bolivia	Anteproyecto de Ley de Protección de datos.	
Brasil	Anteprojeto de Lei de proteção de dados pessoais.	
Chile	Anteproyecto de Ley de protección de las personas en el tratamiento de sus datos personales.	2014
Honduras	Anteproyecto de Ley de Protección de Datos Personales y Acción de Habeas Data.	2014
México	Propuesta de Ley General de Protección de Datos Personales en posesión de sujetos obligados.	2014
Venezuela	Anteproyecto de Ley de Protección de Datos y Habeas Data.	

TENTATIVAS LEGISLATIVAS FALLIDAS

	Proyecto normativo	Año
Ecuador	Proyecto de Ley sobre la protección a la intimidad y los datos personales.	2012
El Salvador	Proyecto de Ley de protección de datos personales.	2010
Venezuela	Anteproyecto de Ley de protección de datos y habeas data.	2004

ORGANISMOS Y AUTORIDADES DE CONTROL

	Órganos nacionales	Otros organismos
Andorra	L'Agència Andorrana de Protecció de Dades.	
Argentina	Dirección Nacional de Protección de Datos Personales.	Dirección de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.
Colombia	Delegatura de Protección de Datos de la Superintendencia de Industria y Comercio.	
Costa Rica	Agencia de Protección de Datos de los Habitantes.	
Ecuador	Superintendencia de Telecomunicaciones.	
España	Agencia Española de Protección de Datos.	Autoritat Catalana de Protecció de Dades. Datuak Babesteko Euskal Bulegoa.
Honduras	Instituto de Acceso a la Información Pública.	
México	Instituto Federal de Acceso a la Información y Protección de Datos.	
Perú	Autoridad Nacional de Protección de Datos Personales.	
Portugal	Comisión Nacional de Protección de Datos.	
Uruguay	Unidad Reguladora y de Control de Datos Personales.	

SUPUESTOS O CONDICIONES PARA EFECTUAR TRANSFERENCIAS INTERNACIONALES DE DATOS

Requisitos generales: ●
Otros supuestos habilitantes: X

Supuestos o condiciones	Andorra	Argentina	Chile	Colombia	Costa Rica	España	México	Nicaragua	Perú	Portugal	Rep. Dominicana	Uruguay	Paraguay	Puerto Rico	Bolivia	El Salvador	Ecuador	Honduras	Panamá	Brasil	Cuba	Guatemala	Venezuela
Nivel de protección adecuado o equivalente	●	●		●		●		●	●	●		●											
Comunicación a la ANPD						●		●	●			●											
Autorización de la ANPD				X		X				X		X											
Consentimiento y/o conocimiento del titular	X	X	X	X	●	X	X	●	●	X	●	●			●								
Obligaciones o condiciones idénticas o similares para el transferente y receptor / Cláusulas contractuales apropiadas					●		X	X	X	X		X											
Información previa al titular							●	●			●												
Cumplimiento de tratados internacionales	X	X	X	X		X	X	X	X		X	X											
Cooperación judicial internacional / Ejercicio o defensa de un derecho	X	X		X		X	X	X	X	X	X	X											
Prevención, diagnóstico, asistencia o tratamientos médicos (interés vital del titular)	X	X		X		X	X	X	X	X	X	X											
Transferencias bancarias o bursátiles	X	X		X		X		X	X		X	X											
Cumplimiento de relaciones jurídicas, contractuales o pre-contractuales	X			X		X	X		X	X	X	X											
Registros públicos con competencia	X	X				X				X	X	X											
Preservación del interés público	X			X		X	X			X	X	X											
Prevista legalmente/ Requerida por autoridad judicial							X								X								

Supuestos o condiciones	**Andorra**	**Argentina**	**Chile**	**Colombia**	**Costa Rica**	**España**	**México**	**Nicaragua**	**Perú**	**Portugal**	**Rep. Dominicana**	**Uruguay**	**Paraguay**	**Puerto Rico**	**Bolivia**	**El Salvador**	**Ecuador**	**Honduras**	**Panamá**	**Brasil**	**Cuba**	**Guatemala**	**Venezuela**
Con destino a sociedades controladoras, filiales o subsidiarias bajo control común del responsable / Matriz o sociedades del mismo grupo del responsable							X		X														
Lucha contra crimen organizado, terrorismos y/o narcotráfico		X						X	X		X	X											
Existencia de cláusulas contractuales tipo (aprobadas por la Comisión Europea)										X													

BIBLIOGRAFÍA

OBRAS CONSULTADAS

ÁLVAREZ DE BOZO, M., PEÑARANDA QUINTERO, F. M., y PEÑARANDA QUINTERO, H. R.: *La Libertad Informática. Derecho Fundamental de la Constitución Venezolana*. Publicaciones Universidad del Zulia y Organización Mundial de Derecho e Informática. Maracaibo, 1999.

ARIAS KRISTY, B. F., CAVALLINI A., QUESADA C., BRIONES L. Profesor del curso Lic. Guillermo Augusto Pérez Merayo. *El* Habeas Data. 2000.

BARINAS UBINAS, B.: «La Protección Jurídica de los Datos Personales en República Dominicana». Encuentro Iberoamericano de Protección de Datos Personales Cartagena de Indias. Colombia. 27-31 mayo, 2008.

BENÍTEZ, L. M.: «La Acción de Habeas Data en el Derecho Paraguayo». *Revista Ius et Praxis,* Universidad de Talca. Año 3 N.º 1. Talca. 1997.

CASTELLANOS KHOURY, J. P.: «Los procesos constitucionales de protección de los Derechos fundamentales en la República Dominicana». Cartagena de Indias, Colombia 3 de diciembre de 2013.

DONEDA, D.: *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

EKMEKDJIAN, M. Á. y PIZZOLO, C.: Habeas data: *El Derecho a La Intimidad Frente a La Revolución Informática,* 1.ª ed, Ediciones Desalma. Buenos Aires. 1998.

GONZÁLEZ M. R.: *El* Habeas Data. Segunda edición, revisada y actualizada. Panamá 2002.

GOZAÍNI O. A.: *Derecho Procesal Constitucional.* Habeas data. *Protección de datos personales. Ley 25.326*. 1.º ed., Rubinzal-Culzoni, Bs.As.. 2002.

JIJENA LEIVA, R.: «La Ley Chilena de Protección de Datos Personales. Una visión crítica desde el punto de vista de los intereses protegidos». *Cuadernos de Extensión Jurídica,* Universidad de Los Andes, N.º 5, 2001.

MARTÍNEZ M. S.: Habeas Data *Financiero*. Ediciones de la República. 2009.

MORALES, A.: *Direito constitucional*. São Paulo: Atlas, 2013.

PIÑAR MAÑAS, J. L. y ORNELAS NÚÑEZ, L. (Coord.).: *La Protección de Datos Personales en México*. México D.F., 2013, Editorial Tirant lo Blanch.

PEYRANO, G. F.: *Régimen Legal de los Datos Personales y* Habeas Data. Lexis Nexis-Depalma. 2002.

PUCCINELLI, O. R.: «El habeas data en el constitucionalismo indoiberoamericano finisecular», en Toricelli, Maximiliano (coord.) *El amparo constitucional: perspectivas y modalidades* (art. 43, CN) Depalma, Bs. As., 1999, P. 249.

PULIDO JIMÉNEZ, M.: *El acceso a la información es un derecho humano,* tomo 2, serie: Ombudsman, México. 2006.

RECIO GAYO, M.: *Esquemas de la Ley de Protección de Datos Personales en Posesión de Datos personales y su Reglamento*. México D.F., 2013, Editorial Tirant lo Blanch.

REMOLINA ANGARITA, N.: *Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012*. Legis editores. Bogotá, noviembre de 2013. ISBN 978-958-767-086-8.

— «Responsabilidad por el tratamiento de los datos personales de clientes, empleados, proveedores y terceros». Capítulo publicado en la obra: *Fundamentos de derecho de los negocios para no abogados*. Ediciones Uniandes y Editorial Temis. ISBN 978-958-35-0930-8.

— «Los derechos de acceso, rectificación, cancelación y oposición en la ley de datos personales y su reglamento». Capítulo publicado en la obra *La protección de datos personales en México*. Editorial Tirant Lo Blanch. ISBN 978-84-9033-679-3, pag, 181-205. México, D.F. 2013.

— «Tratamiento de datos personales en el contexto laboral». Artículo publicado en la *revista Actualidad Laboral y Seguridad Social de Legis*. ISSN 0123-9899. No 175. Bogotá, enero-febrero de 2013.

RODRÍGUEZ MENDOZA, A. M.: «El reto de Costa Rica frente a la institucionalización de la Agencia de Protección de Datos de los Habitantes, PRODHAB, con fundamento legal en la Ley N.º 8968». *Revista Electrónica de la Facultad de Derecho,* ULACIT-Costa Rica. Derecho en Sociedad N.º 3, 2012.

SUÑÉ LLINÁS, E.: *Tratado de Derecho Informático, Vol. I, Introducción y Protección de Datos Personales*. Universidad Complutense. Facultad de Derecho e Instituto Español de Informática y Derecho. Madrid. 2000.

VV.AA.: *Estudio de impacto y comparativa con la normativa de la propuesta de Reglamento General de Protección de Datos de la Unión Europea*. ISMS Forum Spain – DPI. Madrid 22.11.2012.

VV.AA.: *II Estudio del borrador de Reglamento de Protección de Datos «Reflexiones sobre el futuro de la Privacidad en Europa»,* ISMS Forum Spain – DPI. Madrid 6.11.2013.

VILLALOBOS, E. A.: *Introducción a la Informática. Informática jurídica y Derecho informático*. Panamá, 1997.

ZALDÍVAR, K. M.: «El derecho a la intimidad en la Era de la información», *Divulgación Jurídica,* año III, número 5, octubre de 1996.

PÁGINAS WEB DE REFERENCIA CONSULTADAS

— Agencia de Protección de Datos de los Habitantes (Costa Rica)
http://www.prodhab.go.cr/
— Agencia Española de Protección de Datos (España)
https://www.agpd.es/portalwebAGPD/index-ides-idphp.php
— Autoridad Nacional de Protección de Datos Personales (Perú)
http://www.minjus.gob.pe/proteccion-de-datos-personales/
— Autoritat Catalana de Protecció de Dades (España)
http://www.apd.cat/ca/index.php
— Comisión Nacional de Protección de Datos (Portugal)
http://www.cnpd.pt/
— Consejo para la Transparencia (Chile)
http://www.consejotransparencia.cl/consejo/site/edic/base/port/inicio.html
— Datuak Babesteko Euskal Bulegoa (España)
http://www.avpd.euskadi.net/s04-4319/es/
— Dirección de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires (Argentina)
http://www.cpdp.gov.ar/
— Dirección Nacional de Protección de Datos Personales (Argentina)
http://www.jus.gob.ar/datos-personales.aspx
— Grupo Europeo de Protección de Datos del Artículo 29
http://ec.europa.eu/justice/data-protection/index_en.htm
— Instituto de Acceso a la Información Pública (Honduras)
http://www.iaip.gob.hn/
— Instituto Federal de Acceso a la Información y Protección de Datos (México)
http://inicio.ifai.org.mx/_catalogs/masterpage/ifai.aspx
— L'Agència Andorrana de Protecció de Dades (Andorra)
https://www.apda.ad/
— Observatorio Ciro Angarita Barón
http://habeasdatacolombia.uniandes.edu.co/
— Observatorio Iberomaericano de Protección de Datos
http://oiprodat.com/
— Organización de los Estados Americanos
http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp
— Organización para la Cooperación y el Desarrollo Económicos
http://www.oecd.org/

— Parlamento Europeo
http://www.europarl.es/
— Red Iberomaericana de Protección de Datos
http://www.redipd.org/index-ides-idphp.php
— Revista electrónica Habeas Data (Argentina)
http://habeasdatacpdp.wordpress.com/
— Revista Jurídica de la Facultad de Jurisprudencia de la Universidad de Guayaquil
http://www.revistajuridicaonline.com/
— Revista Latinoamericana de Protección de Datos Personales
http://www.rlpdp.com/
— Superintendencia de Industria y Comercio (Colombia)
http://www.sic.gov.co/drupal/
— Superintendencia de Telecomunicaciones (Ecuador)
http://www.supertel.gob.ec/
— Supervisor Europeo de Protección de Datos
http://europa.eu/about-eu/institutions-bodies/edps/index_es.htm
— Unidad Reguladora y de Control de Datos Personales (Uruguay)
http://www.datospersonales.gub.uy/

ÍNDICE DE AUTORES

AUTORES DEL ESTUDIO Y NACIONALIDAD

Argentina
Matilde Susana Martínez
Romina Florencia Cabrera

Bolivia
Édgar David Oliva Terán

Brasil
Cláudio Roberto Santos

Chile
Claudio Ragni Vargas

Colombia
Wilson Rafael Ríos Ruiz

España
Daniel A. López Carballo
Francisco R. González-Calero Manzanares
Javier Villegas Flores
José Luis Colom Planas
Laura Vivet Tañà
Marta Sánchez Valdeón
Ruth Benito Martín
Salvador Serrano Fernández

México
Aristeo García González
Dulcemaría Martínez Ruiz
Héctor E. Guzmán Rodríguez

Nicaragua
Jorge Luis García Obregón

Perú
Cynthia Téllez Gutiérrez

Portugal
João Ferreira Pinto

República Dominicana
Jorge Augusto Tena Ramírez

COORDINADORES DEL ESTUDIO

Coordinador del Estudio: Daniel A. López Carballo
Coordinador Adjunto: Francisco Ramón González-Calero Manzanares

Protección de datos y *habeas data:* una visión desde Iberoamérica

La protección de la privacidad es un derecho fundamental reconocido por las Naciones Unidas que protege la libertad individual, la libertad de expresión, la intimidad y la dignidad personal. El Consejo de Europa lo define como un derecho humano fundamental, la propia Declaración Universal de Derechos Humanos y el Pacto Internacional sobre los Derechos Civiles y Políticos establecen que «nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación».

La mayor parte de Constituciones Iberoamericanas contemplan la especial protección del derecho a la privacidad, al honor y la propia imagen, entre otras, Honduras (1982), Ecuador (2008), Perú (1993) y Paraguay (1992). En las diferentes legislaciones encontramos referencias al *habeas data* como protección del derecho contra la información abusiva, inexacta o perjudicial para las personas, íntimamente ligada al derecho a la protección de datos de carácter personal.

Iberoamérica avanza en la legislación de este derecho fundamental hacia un marco jurídico común que cree un espacio de seguridad jurídica tanto en el ámbito empresarial y las transacciones económicas y de servicios como de la libre circulación de las personas y sus relaciones más allá de su espacio cotidiano.

En una sociedad global, donde internet y las nuevas tecnologías eliminan las barreras físicas, el conocimiento del derecho debe ser global para dar una respuesta adecuada a las necesidades de las personas. El mundo está en movimiento y constante cambio, y el derecho debe seguir esa estela adaptándose a los nuevos tiempos.