Revista de Derecho
FORO
ISSN 1390-2466
Universidad Andina Simón Bolívar, Sede Ecuador
Corporación Editora Nacional

La protección de datos personales en la era digital

27
I semestre 2017

Jurisprudencia

FORO Revista de Derecho

Revista del Área de Derecho
UNIVERSIDAD ANDINA SIMÓN BOLÍVAR
Sede Ecuador

ISSN 1390-2466
Primer semestre de 2017 • Número 27

FORO: revista de derecho recoge trabajos de alto nivel que enfocan problemas jurídicos en los ámbitos nacional, regional e internacional resultantes de los procesos de análisis, reflexión y producción crítica que desarrollan profesores, estudiantes y colaboradores nacionales y extranjeros. *FORO* es una revista del Área de Derecho de la Universidad Andina Simón Bolívar, Sede Ecuador, creada para cumplir con el rol institucional de promoción y desarrollo del conocimiento, cuya dinámica nos exige respuestas innovadoras a las complejas situaciones que se producen cotidianamente.

Director del área: Dr. Ramiro Ávila Santamaría.

Editor de la revista: Dr. Ramiro Ávila Santamaría.

Comité editorial: Dra. Roxana Arroyo Vargas (Instituto de Altos Estudios Nacionales), Dr. Santiago Basabe Serrano (Facultad Latinoamericana de Ciencias Sociales, Sede Ecuador), Dra. Eddy De la Guerra Zúñiga (Universidad Andina Simón Bolívar, Sede Ecuador), Dra. Elisa Lanas Medina (Universidad Andina Simón Bolívar, Sede Ecuador), Dra. Sonia Merlyn Sacoto (Pontificia Universidad Católica del Ecuador), Dr. César Montaño Galarza (Universidad Andina Simón Bolívar, Sede Ecuador), Dr. Marco Navas Alvear (Universidad Andina Simón Bolívar, Sede Ecuador), Dr. Farith Simon Campaña (Universidad San Francisco de Quito).

Comité asesor internacional: Dr. Víctor Abramovich (Universidad de Buenos Aires), Dr. Alberto Bovino (Universidad de Buenos Aires), Dr. Antonio de Cabo de la Vega (Universidad Complutense de Madrid), Dr. Miguel Carbonell (Universidad Nacional Autónoma de México), Dr. Silvio Gambino (Universidad Della Calabria), Dr. Andrés Gil Domínguez (Universidad de Buenos Aires), Dr. Fernando Puzzo (Universidad Della Calabria), Dra. Claudia Storini (Universidad Pública de Navarra), Dr. Víctor Uckmar (Universidad de Génova), Dr. Rodrigo Uprimny (Universidad Nacional de Colombia), Dra. Rosario Valpuesta (†) (Universidad Pablo de Olavide), Dr. Alberto Zelada (Universidad Andina Simón Bolívar, La Paz), Dr. Francisco Zúñiga (Universidad de Chile).

Coordinadores del número: Dra. María Augusta León M. y Mg. Luis Enríquez A.
Coordinadora editorial: Esp. Sup. María José Ibarra González.
Supervisor editorial y diagramación: Jorge Ortega.
Corrección: Fernando Balseca.
Cubierta: Raúl Yépez.
Impresión: Editorial Ecuador, Santiago Oe2-131 y Versalles, Quito.

CORPORACIÓN EDITORA NACIONAL

UNIVERSIDAD ANDINA SIMÓN BOLÍVAR
Ecuador 25 años

FORO aparece en los índices *Latindex: Sistema regional de información en línea para revistas científicas de América Latina, el Caribe, España y Portugal*; *Prisma: Publicaciones y revistas sociales y humanísticas*, y *Latinoamericana: Asociación de revistas académicas de humanidades y ciencias sociales*.
FORO es una publicación gestionada por su comité editorial que circula semestralmente desde noviembre de 2003. Para la selección de ensayos se utiliza el sistema de doble ciego (*peer review*).
Las ideas emitidas en los artículos son de responsabilidad de sus autores. Se permite la reproducción si se cita la fuente.

FORO
Revista de Derecho
ISSN 1390-2466
Universidad Andina Simón Bolívar, Sede Ecuador /
Corporación Editora Nacional
No. 27 • I semestre 2017

FORO
Revista de Derecho
ISSN 1390-2466
Universidad Andina Simón Bolívar, Sede Ecuador /
Corporación Editora Nacional
No. 27 • I semester 2017

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

Editorial

En los últimos años, el vertiginoso avance de las tecnologías de la información y la comunicación han contribuido a la construcción de la sociedad de la información. Esta sociedad sin fronteras ha permitido el acceso e intercambio de información en tiempo real, generando redes globales de conocimiento. Por otro lado, este avance ha descubierto la sensibilidad del tratamiento de nuestros datos personales. Considerando la importancia de la protección de datos en la sociedad de la información, este número de la Revista de Derecho FORO *está dedicado a impulsar la discusión sobre el desarrollo de la legislación en relación a la protección de datos personales.*

Un primer eje de análisis se concentra en el papel del derecho en la reglamentación de datos personales. El artículo titulado "De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales", escrito por Claudia Orellana Robalino, expone la ineficiencia de la seguridad informática en la protección de datos personales y la necesidad de un cambio de visión hacia la resiliencia cibernética. En esta misma línea, el artículo de Andrea Villalba Fiallos, "Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa", reflexiona sobre la importancia del desarrollo del derecho y las políticas públicas en el fortalecimiento del derecho a la intimidad y su vinculación con la protección de datos.

Un segundo eje de discusión se focaliza en la protección de datos en Ecuador. El artículo "Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales", de Luis Enríquez Álvarez, subraya la necesidad de la adopción de una regulación a nivel nacional que cumpla los estándares mínimos de tratamiento y transferencia de datos para proteger el derecho a la vida privada de los ecuatorianos, y como requisito para el surgimiento de emprendimientos ecuatorianos en internet. Por otro lado, Lorena Naranjo en su artículo "El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador" critica la postura jurisprudencial ecuatoriana frente al carácter informativo que debe tener el dato personal para configurarse como presupuesto del derecho de protección de datos.

En un tercer eje, la revista FORO *presenta dos artículos que analizan la protección de datos desde una visión regional e internacional. El artículo de Luis Ordóñez*

Pineda, "La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración" analiza el desarrollo del derecho de autodeterminación en el contexto de la Comunidad Andina y promueve la idea de un modelo interamericano para la regulación del tratamiento de datos personales. Desde una visión europea, Marcel Moritz y Valentin Gibello exponen, en su artículo "El Reglamento Europeo (UE) 2016/679: Análisis de un claroscuro", los retos que enfrenta el nuevo Reglamento europeo sobre protección de datos personales (UE) 2016/679 en el fortalecimiento de la protección de datos personales en este continente.

Finalmente, el número concluye con un interesante análisis jurisprudencial en relación al derecho al olvido. A través del caso Perú vs. *Google. Alexander Cuenca Espinosa enfoca la vinculación del derecho al olvido con derecho a la defensa y la libertad de expresión. Cierra este número el análisis jurisprudencial comparado de los casos Google* vs. *España y Gloria* vs. *El Tiempo, realizado por María Gabriela Espinoza.*

Esta nueva entrega de la Revista de Derecho FORO *busca ser una plataforma para la discusión y reflexión sobre un tema tan novedoso y a la vez sensible como la regulación de la protección de datos personales a nivel nacional, regional y global.*

María Augusta León Moreta
Luis Enríquez Álvarez

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales

*Claudia Orellana Robalino**

RESUMEN

Las tecnologías de la información y comunicación nos permiten vivir en una sociedad en red, sin embargo, existen varios riesgos de la hiperconectividad, tales como la seguridad de la información, y parte de esta son los datos personales. Este reto se afrontó desde la visión de la seguridad cibernética, que protege el proceso de tratamiento de la información y la seguridad de los sistemas de información; no obstante, una vez vulnerado, los recientes ataques a las redes de información públicas y privadas han demostrado la ineficiencia de la seguridad cibernética. Por esto el Foro Económico Mundial publicó en 2017 los principios de resiliencia cibernética avanzada, que constituyen un cambio en la visión de la seguridad cibernética a la resiliencia cibernética, indicando que la seguridad debe ser preventiva, siendo sus objetivos principales: orientar la gobernanza de la información desde el órgano de gobierno, y garantizar la veracidad e integridad de los datos personales, siendo delimitados por principios legales que permiten la protección de los mismos y el cumplimiento del Derecho a la protección de datos personales y la vida privada.

Palabras clave: resiliencia cibernética, protección de datos personales, derecho a la privacidad, seguridad cibernética, tecnologías de la información y comunicación.

ABSTRACT

Information and communication technologies allows us to live in a network society, however there are several risks of a hyperconectivity, one of them is the safety of the information; some of these information is personal data. This challenge was assumed by the cyber security vision, which protects the treatment of information and information security systems once is violated, however the recent attacks on public and private information systems, have shown the inefficiency of cyber security, this is why the World Economic Forum published in 2017 Advancing cyber

* Asesora legal de la Universidad de las Américas (UDLA).

resilience principles and tools for boards, that has changed the vision from cyber security to cyber resilience, indicating that security must be preventive, which main objectives are to guide the governance of the information from the executive body or boards of directors, guarantee the accuracy and integrity of the personal data, and to achieve these, institutions must apply legal principles that allow protection and the fulfilment of data protection and private life rights

KEYWORDS: cyber resilience, personal data protection, right of privacy, cyber security, information and communication technologies.

FORO

INTRODUCCIÓN

El presente ensayo es explicativo, descriptivo y argumentativo, y pretende demostrar la necesidad de la inclusión de los principios de resiliencia cibernética avanzada del Foro Económico Mundial de 2017 en el ordenamiento jurídico ecuatoriano, o en políticas públicas o privadas para promover la gobernanza de la información, que incluye la protección de datos personales. El ensayo está compuesto de tres argumentos:

1. El derecho a la protección de los datos personales y su conexión con el derecho a la vida privada y a la información. Aquí se señala que la tendencia europea y latinoamericana es considerar e interpretar al derecho a la protección de datos personales como parte del derecho a la vida privada, se indica la relación entre el derecho de acceso a la información, que es la regla general, y la protección de datos personales que es la excepción, y se menciona que el hábeas data es el recurso idóneo para el ejercicio del derecho a la protección de datos personales.
2. Análisis de casos internacionales: el caso Evans *vs.* Reino Unido del año 2000, la sentencia del Tribunal Europeo de Derechos Humanos (TEDH), y del caso No. 1894 del año 2011, resuelto por el Tribunal Constitucional de Chile, que manifiestan la importancia del derecho a la protección de datos personales y su alcance a la información circulante en internet.
3. En el argumento final se realiza un análisis del cambio de la seguridad cibernética a la resiliencia cibernética y se enfatiza en la importancia de los principios de resiliencia cibernética del Foro Económico Mundial de 2017.

EL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES Y SU CONEXIÓN CON EL DERECHO A LA VIDA PRIVADA FAMILIAR Y A LA INFORMACIÓN

Derecho de acceso a la información como regla general

El derecho de acceso a la información es un derecho incluido en la libertad de expresión, que ha sido reconocido en varios instrumentos internacionales de derechos humanos, tales como: art. 9 de la Declaración Universal de Derechos Humanos, 1948 (DUDH); art. 19 del Pacto Internacional de Derechos Civiles y Políticos, 1969 (PIDCP); art. 13 de la Convención Americana de Derechos Humanos, 1969 (CADH); entre los principales. Es considerado un derecho que permite el ejercicio de la democracia, de la participación ciudadana, y es un mecanismo de control del Estado por parte de los ciudadanos para verificar el cumplimiento de su gestión y funciones públicas. En consecuencia, el derecho de acceso a la información es "una herramienta crítica para el control del funcionamiento del Estado y la gestión pública, y para el control de la corrupción",[1] y se rige por dos principios:[2]

1. Máxima divulgación: la regla general establece que todas las personas tienen derecho al acceso a la información en posesión de órganos públicos. La excepción es el secreto, pero la regla general es la máxima divulgación.
2. Buena fe: el Estado debe actuar de buena fe para permitir el ejercicio de derecho al acceso a la información, para lo cual debe garantizar recursos efectivos que permita el ejercicio del derecho a la información. Además de garantizar dicho recurso, las obligaciones del Estado incluyen: i) interpretar leyes en favor de este derecho; ii) brindar asistencia para el ejercicio de este derecho; iii) actuación con transparencia de los funcionarios públicos para que realicen las acciones necesarias para garantizar el interés general.[3]

---

1. Comisión Interamericana de Derechos Humanos, *El derecho al acceso a la información en el marco latinoamericano*. OEA Serie L/V/II CIDH/RELE/INF.9/12, 2012 párr. 5, 2.
2. Estos principios han sido reconocidos en diferentes instrumentos internacionales como los Principios de Lima, Principios de Johannesburgo sobre la Seguridad Nacional, 10 Principles on the right to know OAS.
3. Comisión Interamericana de Derechos Humanos, *El derecho al acceso a la información en el marco latinoamericano.* OEA Serie L/V/II CIDH/RELE/INF.9/12, 2012 párr. 17.

Derecho a la protección de la vida privada como libertad de autonomía

El derecho a la vida privada es un derecho fundamental reconocido en los principales instrumentos de Derechos humanos, tales como el art. 12 de la DUDH, art. 17 del PIDCP y art. 11 de la CADH, entre los principales, cuyo objetivo es proteger la vida privada y permitir el ejercicio de la libertad de autonomía de cualquier injerencia externa arbitraria o ilegal que pueda afectar o afecte la dignidad de la persona. Para Juan Carlos Hernández, el derecho a la protección implica tres aspectos fundamentales: "1. Derecho a disfrutar una vida privada libre. 2. El derecho a comunicarse libremente con cualquier persona sin el temor a ser vigilado. 3. El derecho a controlar el acceso a la información personal".[4]

En esta perspectiva, el derecho a la protección de datos personales o autodeterminación de la información estaría contenido en el derecho a la protección a la vida privada y familiar. Sin embargo, existen nociones que consideran que el derecho a la protección de datos personales es independiente del derecho a la vida privada. Esta diferencia dependerá de la legislación de cada país. En la Unión Europea y en Latinoamérica de forma general se aplica el criterio de considerar el derecho a la protección de datos personales como parte del derecho a la privacidad, mientras que en Estados Unidos el derecho a la protección de datos es independiente, porque existen datos personales que pueden ser compartidos a terceros sin mayor riesgo a que atente contra su vida privada.

En consecuencia, no existe una ley específica de datos personales, ya que hay un modelo de protección más flexible que permite la autorregulación y el control de los datos personales de conformidad con el sector e industria que los maneja, tales como bancos, compañías de e-comerce, universidades, proveedores de servicios de internet, entre otros.[5] Sin embargo, existen datos sensibles como aquellos contenidos en la historia clínica de pacientes, o datos proporcionados por menores de edad en internet, entre los más importantes, que son regulados por leyes específicas.[6]

---

4. Juan Carlos Hernández, "La protección de datos personales en internet y el hábeas data", *Revista derecho y tecnología*, No. 13 (2012): 62.
5. Lisa Soto, Aron Simpson, *Data Protection & privacy 2015 in United States* (Reino Unido: Law Business Research, 2015), 208.
6. Health Insurance Portability and Accountability Act de 1996 (HIPPA) es una ley de carácter federal que delimita el uso, la divulgación y protección de los datos médicos de las personas. Children's Online Privacy Protection Act (COPPA) protege los datos personales recolectados en línea de los menores de 13 años, imponiendo obligaciones a las instituciones que los recolectan, almacenan y utilizan.

Derecho a la protección de datos personales o autodeterminación de la información

El derecho a la protección de datos personales o autodeterminación de la información tiene sus orígenes en 1970, cuando países europeos empiezan a dictar leyes que regulan la protección de datos personales, pero con el objetivo de regular las tecnologías y, específicamente, las bases de datos de información; no obstante, estas legislaciones fueron modificadas y el derecho a la protección de datos personales fue interpretado a la luz del derecho a la privacidad.[7]

Algunas legislaciones tales como la Data Protection Act de 1998 de Reino Unido, Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal de España, y la Ley Estatutaria 1581 de 2012 de Colombia coinciden en que existen principios que rigen la protección de datos personales:

- Consentimiento informado: para la recolección, el almacenamiento, el uso, la modificación o eliminación de los datos personales es indispensable contar con el consentimiento del titular de forma expresa.
- Confidencialidad de acceso y circulación restringida: los datos personales siempre son confidenciales, excepto que exista el consentimiento o la autorización judicial para divulgarlos. La autorización judicial se aplica en los casos que exista una lesión, fundamentada en las libertades o derechos de otras personas, que se conoce como principio de lesividad.
- Legalidad: el tratamiento de los datos personales estará sujeto a las normas legales.
- Justificación, pertinencia y no exceso: no podrán recolectarse y usarse datos personales para finalidades incompatibles con aquellas para que los datos hubieran sido recogidos, tampoco puede recolectarse de manera excesiva, ilegal o fraudulenta los datos; debe hacérselo únicamente para el fin específico que se recolecta.
- Acceso a los datos personales: el titular de los datos personales tendrá acceso en cualquier momento a sus datos personales, para autorizarlos, rectificarlos, modificarlos o eliminarlos.
- Plazo de almacenamiento: el tratamiento de los datos personales debe estar sujeto a un plazo.

---

7. Francisco Gonzales Hoch, "Privacidad de la información digital: autodeterminación *vs.* Commodity", *Revista jurídica de la Universidad de Palermo*, No. 7 (2010): 79.

- Seguridad: el encargado del tratamiento de los datos personales, sea una institución pública o privada, garantizará a través de medidas técnicas, administrativas, entre otras, la seguridad de los sistemas que contengan los datos personales, para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

El mecanismo legal idóneo para garantizar el ejercicio del derecho a la protección de datos personales es el hábeas data, una garantía constitucional que "protege el derecho que tiene la persona al acceso y conocimiento de sus datos personales en registro públicos y privados".[8] En la actualidad la tendencia jurídica es considerarlo un proceso autónomo del amparo constitucional, ya que "presenta caracteres propios y peculiaridades morfológicas que la hacen merecedora de un tratamiento normativo también singular e individual".[9]

Al utilizar el mecanismo legal del hábeas data se ejerce el derecho a la información, pero de forma específica, porque es un instrumento que permite a las personas conocer la información propia contenida en bases de datos públicas o privadas con el objetivo de autorizarla, modificarla, rectificarla o eliminarla para de esta forma ejercer el derecho a la protección de datos personales. El objeto del hábeas data es toda la información personal que se encuentre bajo custodia, administración o tenencia del Estado o institución privada, mientras que el objeto del derecho a la información es más amplio, porque es aquel que se encuentre bajo custodia del Estado, al respecto se señala que "se refiere a toda la información en bases de datos públicas significante, cuya definición debe ser amplia, incluyendo toda la que es controlada o archivada en cualquier formato y medio".[10]

---

8. Hernández, "La protección de datos personales en internet y el hábeas data", 69.
9. Víctor Bazán, "El hábeas data, su autonomía respecto del amparo y la tutela del derecho fundamental a la autodeterminación normativa", *Anuario de Derecho Constitucional Latinoamericano*, No. 37 (2012): 66.
10. Comité jurídico interamericano de la OEA, *Principios sobre el acceso al derecho a la información*. OEA, 2008, 1.

ANÁLISIS DE CASOS A NIVEL INTERNACIONAL Y REGIONAL RELACIONADOS A LA PROTECCIÓN DE LOS DATOS PERSONALES

Case Brief: Rol 1894 de 12 julio 2011 Tribunal Constitucional de Chile

En Chile se aprueba en 2011 la Ley 20526 que sanciona el acoso sexual de menores, la pornografía infantil y la posesión de material pornográfico. Antes de la promulgación y publicación de la Ley 20526 está contenía el art. 4 que señalaba: "Los establecimientos comerciales, cuya actividad principal sea ofrecer al público servicios de acceso a internet, a través de computadores propios o administrados por ellos, deberán mantener un registro actualizado de los usuarios".[11] El Congreso Nacional (CN) solicita al Tribunal Constitucional de Chile (TCC) que realice el control preventivo de constitucionalidad del art. 4 del proyecto de ley 20526, ya que la mayoría de diputados consideran que el art. 4 atenta contra el derecho a la vida privada de las personas y la protección de sus datos personales al tenor de los dispuesto en el art. 19, No. 4[12] de la Constitución chilena.

Así, el TCC concluye que, a pesar de que la ley tiene el fin de proteger a la infancia de delitos como el acoso sexual y la pornografía infantil, el proyecto de Ley en su art. 4 es inconstitucional y debe eliminarse su texto, porque la implementación de un registro de datos personales recolectados de los cibercafés es violatoria de varios derechos, resolviendo:

1. La creación de un registro de datos personales sin el consentimiento de la persona no es válido, porque la persona no autoriza la recolección, el uso, el almacenamiento, la modificación ni destrucción de los datos.
2. La interferencia válida en la vida privada de la persona sería en los casos previstos por la Ley, para precautelar la seguridad nacional, derechos y libertades fundamentales y el orden público; en tales casos debe existir una autorización judicial para la recolección, almacenamiento y uso de los datos personales.
3. La vigilancia y monitoreo constantes de los usuarios, a través de los datos personales recolectados de internet (sitios web que se visita, la frecuencia, las direcciones de correo con quien contacta, redes sociales, correo electrónico entre

11. Proyecto de Ley que sanciona el acoso sexual de menores, la pornografía infantil y la posesión de material pornográfico.
12. Constitución de la República de Chile, art. 19, No. 4 "El respeto y protección a la vida privada y a la honra de la persona y su familia".

otros) generan perfiles sociales, de hábitos, preferencias comerciales, ideología política e inclinaciones sociales de las personas monitoreadas.

4. Esta vigilancia ocasionaría un compartimiento inhibitorio, basada en el conocimiento de que los datos personales están siendo revisados en el momento de acceder a los cibercafés, atentando de esta manera contra la libertad personal, la vida privada, la protección de datos personales que, en conjunto, permiten el desarrollo de la personalidad respetando su dignidad humana.
5. La vida privada se ejerce también en lugares de acceso público como es el caso de los cibercafés, que, a pesar de estar abiertos a todo público, se organizan en cabinas individuales y reservadas para garantizar la privacidad de la persona.
6. Lo mismo sucede con internet que, a pesar de ser una red mundial, los datos personales que transitan son considerados confidenciales, a menos que la persona autorice su divulgación.
7. Imponer la obligación de recaudar datos a los cibercafés y de resguardarlos sin las debidas medidas de seguridad es riesgoso para la confidencialidad de los datos personales, porque al existir la posibilidad de que sean utilizados con fines de investigación policial su recolección y seguridad no debe ser encomendada a particulares.

Case Brief: Copland *v.* The United Kingdom sentencia del TEDH 2006

La señorita Copland en 1991 inició su trabajo en Carmarthenshire College (El Colegio), que es una institución pública de educación en Reino Unido. A finales de 1995 se requirió que trabajara para el subdirector. En 1998 la señorita Copland se enteró de que el subdirector había ordenado una investigación, monitoreo y vigilancia únicamente a ella, que incluyó: i) De su teléfono: lista de llamadas recibidas, contestadas, marcadas y su duración. ii) Del correo electrónico institucional: mensajes recibidos, enviados y direcciones de correo. iii) Uso del internet: se revisaron los sitios web que visitaba, la frecuencia con que lo hacía y las fechas en las que realizó las visitas.

Por estos motivos, pidió la aplicación de la Ley de protección de datos personales de 1984 "Data Protection Act 1984" (1984 Act), la cual indica que, en caso de recolección no autorizada de datos personales, la persona afectada podrá solicitar la compensación por daños y perjuicios.[13] A su vez, "The 1984 Act" establece que es una

13. Sección 23 "The 1984 Act".

contravención penal el no cumplimiento de los principios de la protección de datos y que la persona que haya incumplido será notificada con la respectiva sanción, y, en caso de incumplimiento de dicha sanción, será considerado delito.

En el presente caso, la Corte considera que se aplica de forma parcial los principios 1, 2,4 de la "1984 Act",[14] porque se obtienen de manera no autorizada los datos personales contenidos en correos electrónicos, datos de internet y llamadas de Copland, pero la obtención de estos datos sí tiene un propósito específico, que es demostrar si los recursos de una institución pública son usados de forma correcta, es decir para fines de trabajo y no personal, además la recolección de los datos personales no es de forma excesiva, pues la vigilancia que se hace es solamente de fechas, duración de llamadas, páginas que visita y direcciones de correo a las que envía y de las cuales recibe, mas no del contenido de las llamadas, mensajes o de la página web. Por lo tanto, la Corte en Reino Unido determina que no existe la violación de los datos personales de Copland, pero que, al no existir la autorización de ella, el Colegio incurre en una contravención penal, mas no en un delito.

La Srta. Copland inició el proceso ante el Tribunal Europeo de Derechos Humanos (TEDH), con la pretensión que se declare la violación de su derecho a la vida privada y familiar (art. 8) y su derecho a un recurso efectivo (art. 13) reconocidos en el Convenio Europeo de Derechos Humanos.

Resolución de fondo

Después de analizar tanto el caso como el Convenio Europeo de Derechos Humanos, el TEDH concluye:

1. Las llamas telefónicas, el correo electrónico y el uso del internet realizado desde el lugar de trabajo o negocio son considerados parte de la vida privada de una persona.
2. Que la señorita Copland no fue advertida en ningún momento que sus llamadas, correos y uso de internet iban a ser monitoreados.

---

14. Los principios 1, 2,4 "1984 Act" son: 1. la información que contengan datos de carácter personal deberá ser obtenida y procesada, de forma justificada y legal. 2. La recolección de datos personales se realizará para propósitos específicos o legalmente autorizados. 4. La recolección de datos personales para cualquier propósito será obtenida de forma adecuada, pertinente y no excesiva en relación con el propósito que se busca cumplir. Texto original: disponible en ‹http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf›. Mi traducción.

3. El TEDH analiza si dicha interferencia fue acorde a la Ley. El TEDH considera que, al no existir una ley, al momento de los hechos, que regule la vigilancia y monitoreo de medios de comunicación dentro de una institución pública y privada, así como la inexistencia de la facultad de vigilancia y monitoreo en el reglamento de funcionamiento del colegio, ni de ninguna política interna, tal interferencia no fue acorde a la Ley. En consecuencia, el TEDH considera que la recolección y el almacenamiento de información personal relativa al teléfono, así como a su correo electrónico y el uso de internet de Copland sin su conocimiento, constituye una interferencia al derecho al respeto de su vida privada, que incluye la violación a sus datos personales, derecho reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos.

Así, tras analizar ambas sentencias se infiere que en el caso Copland existe una violación directa a los datos personales contenidos en los canales de comunicación institucional, mientras que el argumento del TCC chileno concluye que pudiere existir una violación de los datos personales circulantes en el internet de los usuarios de cyber cafés.

Por tanto, en ambos casos no existe el consentimiento expreso del titular de los datos personales para la recolección, el uso, el almacenamiento y el tratamiento de los mismos, demostrando la ligereza con la que se procede sobre la seguridad cibernética de los datos personales, ya que en ambos casos no se toma en cuenta el principio de seguridad, por lo que su consulta es de manera arbitraria al acceder de forma libre a los servidores donde se encuentran almacenados sin una orden judicial o autorización previa del titular, irrespetando los principios de confidencialidad, consentimiento informado y seguridad cibernética.

PRINCIPIOS DE RESILIENCIA CIBERNÉTICA PARA LA PROTECCIÓN DE DATOS PERSONALES

Principales antecedentes de los principios de resiliencia cibernética

La noción de resiliencia cibernética está presente desde el Foro Económico Mundial de 2011. Con la actualización de la ISO/IEC 27001 de 2013 por la Organización Internacional de Normalización (ISO por sus siglas en inglés)[15] se implementó que la seguridad cibernética abarca el análisis de posibles riesgos.

15. La Organización Internacional de Normalización, es una institución autónoma, con sede en Gine-

Antes de analizar los principios de resiliencia cibernética, a continuación se analizan los antecedentes más importantes:

1. Normas ISO/IEC 27000: su objetivo principal es el desarrollo de normas generales para el sistema de gestión de seguridad de la información (ISMS por sus siglas en inglés). Estas normas son implementadas por el órgano de la seguridad de la información encargado de la dirección y el control de las actividades del ISMS, que se encuentra subordinado al órgano de gobierno. Esta familia de normas está compuesta por varias, entre ellas, la ISO/IEC 27001.
2. Normas ISO/IEC 27001 de 2013: reemplaza a la norma ISO/ICE 27001 de 2005 y su objetivo principal es establecer los estándares mínimos del modelo de los sistemas de gestión de seguridad de la información (ISMS). Señala que el objetivo de los ISMS es preservar al menos tres cualidades esenciales de la información que son: confidencialidad, integridad y disponibilidad de la información.[16] Esta norma establece el modelo de ISMS, que puede ser modificado según las necesidades de cada organización, pero es importante que el ISMS sea parte integrante de los procesos y la estructura de gestión global y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles.
3. En Ecuador, el Instituto Nacional Ecuatoriano de Normalización (INEN) es el organismo técnico del Sistema Nacional de Calidad, que forma parte de la Organización Internacional de Normalización (ISO), por lo que en 2016 adoptó la ISO/IEC 27000 sobre los ISMS, que señala los parámetros generales para resguardar la información, que incluye los datos personales sea en instituciones públicas o privadas. El proceso para obtener la acreditación de la ISO/IEC 27000 se hace directamente ante el INEN.

---

bra, Suiza, que promueve el uso de estándares internacionales; su objetivo principal es establecer estándares de calidad, fiabilidad, consistencia y seguridad en la producción de bienes y servicios. La mayoría de países latinoamericanos son miembros de la organización a través de sus instituciones encargadas de la normalización. Ecuador es miembro y actúa mediante el Instituto Ecuatoriano de Normalización (INEN). Organización Internacional de Normalización, 2014, ‹http://www.iso.org/iso/home/about/the_iso_story.htm›.

16. i) Confidencialidad: la información no debe ser divulgada a terceros sin el consentimiento del titular o de conformidad con la ley. ii) Integridad: exactitud o fidelidad de la información. iii) Disponibilidad: o accesibilidad a la información solo por los titulares o las entidades autorizadas. ISO/IEC 2700, 2016, ‹https://www.iso.org/obp/ui/#iso:std:66435›.

De la seguridad cibernética a la resiliencia cibernética: principios de resiliencia cibernética avanzada

Estos principios fueron discutidos y redactados en el Foro Económico Mundial[17] de 2017, más conocido como el Foro de Davos, y son el resultado de uno de los debates más importantes que se suscitaron en 2017 en el marco de este Foro, que fue la economía y sociedad digital. Estos principios fueron desarrollados en colaboración con The Boston Consulting Group y Hewlett Packard Enterprise.

La resiliencia cibernética es un cambio en la visión de la seguridad cibernética, que ya no solo implica la mitigación de riesgos y vulnerabilidades o incidentes que ocurren en una red de información o de cualquier tipo; incluye la prevención de estos, la seguridad de la red en sí misma y su conexión con otras redes internas o externas, protegiendo de esta manera a uno de los activos más importantes de una institución: la información, que incluye los datos personales de los inversionistas, accionistas, colaboradores, clientes y personas con quién se tiene relaciones comerciales o de cualquier otra índole.

Las ideas esenciales para comprender la resiliencia cibernética son:

1. El rol de los Estados es vital para promover políticas de resiliencia cibernética.
2. Los líderes de organizaciones deben tener una visión más allá de la seguridad cibernética para construir toda una estrategia y cambio de la cultura organizacional a largo plazo de seguridad de todo el sistema, entendida como la resiliencia cibernética.

Por lo tanto, es indispensable el diálogo entre los diferentes actores de la sociedad en red[18] para generar seguridad, certeza y transparencia en desarrollo de la vida económica y social.[19] En consecuencia, el documento sobre principios de resiliencia

---

17. El Foro Económico Mundial es una organización privada sin fines de lucro, constituida en Suiza, que se reúne anualmente desde 1971, conformada por los principales líderes empresariales, líderes políticos internacionales y periodistas e intelectuales selectos para analizar los problemas más relevantes que afronta el mundo. World Economic Forum, *Foundation Statutes*. Reforma al 2006, art. 3.
18. Los actores de la sociedad en red son: i) los usuarios; ii) proveedores de servicios de internet que incluyen los proveedores de acceso a internet, desarrolladores de aplicaciones y de software, proveedores de servicios de cloud computing, entre los más relevantes; iii) proveedores de infraestructura de internet; iv) proveedores de contenido de internet. Ver Horacio Fernández, *Manual de Derecho informático* (Buenos Aires: FEDYE, 2014), 29-30.
19. "El término sociedad en red fue acuñado en 1991 por el holandés Jan Van Dijk para definir una forma de sociedad que se organiza en redes, y son estas redes sociales las que están configurando hoy en día de forma principal la organización y las estructuras más importantes de la sociedad". Patricia Reyes, *Ciudadanas 2020* (Santiago de Chile: Instituto Chileno de Derecho y Tecnologías, 2011), 196.

cibernética avanzada es una de las herramientas que los participantes del Foro de Davos han solicitado para promover la seguridad cibernética a través de la resiliencia cibernética, cuyo objetivo es combatir los riesgos cibernéticos que van en aumento exponencial, conforme la mayor cantidad de dispositivos electrónicos que se conectan a las varias redes de información existentes que afecta a millones de personas, quienes de forma constante están consumiendo y alimentando las redes con información de todo tipo, entre ellas datos personales.

Los principios de resiliencia cibernética avanzada son el marco de las estrategias de gobernanza de la información para los altos órganos de gobierno de una institución pública o privada que opere en un sistema conectado a una red privada, pública o internet y que pretenda proteger sus activos, entre ellos, la información propia o de un tercero.

Estos principios están conformados por cuatro elementos diferentes, pero interrelacionados entre sí::

1. Principios de resiliencia cibernética para la gobernanza de la información.
2. Principios de herramientas cibernéticas.
3. Marco de riesgos cibernéticos.
4. Guía para los riesgos emergentes tecnológicos.[20]

En el presente ensayo se hace énfasis en *los principios de resiliencia cibernética para la gobernanza de la información*, que están dirigidos a los altos órganos de gobierno de una institución, porque son los principales encargados de implementar la resiliencia cibernética para la protección de sus redes y sistemas de información, a través de la toma de decisiones y la generación de políticas.[21] Es un marco de diez principios que pretenden orientar a los órganos de gobierno de una institución para implementar la resiliencia cibernética como estrategia de la gobernanza de la información. Estos son:

1. Responsabilidad por la resiliencia cibernética: el órgano de gobierno de una institución asume la responsabilidad de la gobernanza de la información, es decir, de decidir e implementar políticas para la resiliencia cibernética. La res-

---

20. World Economic Forum, the Boston Consulting Group y Hewlett Packard Enterprise, colaboradores, *Advancing cyber resilience principles and tools for boards* (Ginebra: World Economic Forum, 2017), 7.
21. Antes de la redacción y adopción del documento se investigaron varias empresas y se obtuvo que el 84% de los directivos encuestados coincidió en que es indispensable contar con directrices y mejores herramientas de resiliencia cibernética para apoyar su trabajo de gobernanza de la información. World Economic Forum, the Boston Consulting Group y Hewlett Packard Enterprise, colaboradores, *Advancing cyber resilience principles and tools for boards*, 6.

ponsabilidad de supervisión y control de cumplimiento puede ser delegada a órganos de menor jerarquía ya existentes o creados para esa función.

2. Instrucción de los miembros: del órgano de gobierno y de los órganos de supervisión en materia de resiliencia cibernética, mediante el asesoramiento y asistencia continua de expertos independientes en materia de resiliencia cibernética, tendencias de amenazas recientes y de seguridad cibernética.
3. Existencia de un oficial de resiliencia cibernética: con suficiente experiencia, autoridad y recursos, quien estará encargado de informar sobre la capacidad de la institución para gestionar la resiliencia cibernética y de monitorear los progresos en la aplicación de metas de resiliencia cibernética.
4. Integración de la resiliencia cibernética: el órgano de gobierno deberá garantizar que el órgano administrativo integrará los principios de resiliencia cibernética avanzada en toda la institución, sus procedimientos internos y externos, en la estrategia general y asignará los recursos necesarios, así como el presupuesto para la implementación de la estrategia de resiliencia cibernética.
5. Tolerancia por el riesgo: el órgano de gobierno anualmente definirá y cuantificará la tolerancia en relación a la existencia de riesgos cibernéticos en la institución, para lo cual deberá ser informada sobre los riesgos actuales y futuros, así como de los requisitos regulatorios para la prevención y mitigación de los riesgos.
6. Evaluación de riesgos y presentación de informes: el órgano de gobierno deberá aprobar la evaluación de riesgos y presentación de informes de conformidad con el marco de riesgos cibernéticos
7. Planes de resiliencia cibernética: el órgano de gobierno debe asegurarse que el órgano de administración brinde suficiente soporte al oficial de resiliencia cibernética, a través de planes de resiliencia cibernética, que incluya la creación, implementación, pruebas y continua mejora de la estrategia de resiliencia cibernética. El oficial a cargo deberá supervisar el rendimiento e informar regularmente al órgano de gobierno.
8. Trabajo en conjunto: el órgano de gobierno debe promover el trabajo en conjunto entre el oficial y los colaboradores de la institución a fin de asegurar la resiliencia cibernética.
9. Revisión: el órgano de gobierno debe asegurar que se realice una revisión anual de forma formal e independiente de los planes de resiliencia cibernética.
10. Eficacia: el órgano de gobierno deberá revisar de forma periódica su propio rendimiento y el de la organización en cumplimiento de la planificación de resiliencia cibernética, para esta revisión se puede requerir el asesoramiento externo de un experto.

CONCLUSIONES

Derecho a la protección de datos contenido en el derecho a la vida privada

La protección de los datos personales se encuentra contenida en el derecho a la vida privada, ya que existe una evidente relación entre ambos derechos que son personalísimos, y tienen como objetivo la protección de la esfera privada de los individuos y su desarrollo de forma libre sin ningún tipo de injerencia no autorizada. Así mismo, los casos analizados en el punto dos de este ensayo demuestran que la tendencia general tanto de Europa como Latinoamérica es interpretar y considerar el derecho a la protección de datos personales comprendido como parte de la protección a la vida privada, ambos derechos se relacionan con el derecho a la información, porque la regla general es que todos tienen acceso a la información, y una de sus excepciones son los datos personales, que solo se puede acceder si existe el consentimiento informado de la persona o con autorización judicial, demostrando así que el derecho a la vida privada y a la protección de datos personales no es absoluto, pues hay casos en los que cabe aplicar el principio de lesividad para acceder a datos personales. A su vez, se considera que el mecanismo legal idóneo para el ejercicio del derecho a la protección de los datos personales es el de hábeas data, ya que actúa como garantía constitucional del derecho a la protección de datos, permitiendo a las personas acceder a la información que se encuentra contenida en registro públicos y privados para poder autorizarla, ratificarla, modificarla o eliminarla.

Datos personales contenidos en redes de información

Del análisis de los casos del punto dos del ensayo se infiere que los datos personales que circulan en la red más amplia de información llamada internet, tales como las direcciones de las páginas web que se visitan, el acceso al correo electrónico, las redes sociales que se utilizan y los servicios de internet como las aplicaciones, cloud computing, entre otros, contienen datos personales que no están sujetos a vigilancia y monitoreo, debido a que se atentaría contra el derecho a la protección de datos personales y a la vida privada, pues de la vigilancia de estos datos se generan perfiles sociales, de hábitos, preferencias comerciales, ideología política e inclinaciones sociales de las personas monitoreadas. En cuanto a las redes privadas, como es el caso de las redes institucionales, públicas o privadas, es imprescindible contar con políticas claras que manifiesten que la red compuesta por diferentes canales de comunicación, como el correo institucional, los chats institucionales y los datos de navegación, serán sujetos

a vigilancia y monitoreo para verificar que no sean utilizados con fines personales, pero en esos casos la vigilancia estaría autorizada.

Principios de resiliencia cibernética como lineamientos para garantizar la seguridad de los datos personales y promover la gobernanza de la información

Los principios de resiliencia cibernética y los principios del derecho a la protección de datos personales pueden ser los lineamientos para la creación de una norma, política pública o política privada que regule el tratamiento de los datos personales y los proteja de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; así mismo, pueden ser utilizados como estándares para la gobernanza de la información. Si bien existen estándares normalizados para la protección de los ISMS basados en la visión de la seguridad cibernética de mitigar las vulnerabilidades, riesgos o incidentes ya ocurridos, como es el caso de la ISO/ICE 27000 y sus derivadas, han demostrado ser ineficientes; porque las estrategias, políticas y planes de seguridad de la información deben, a más de mitigar incidentes, promover la prevención de estos, para lo cual se requiere un cambio de visión, que exige que se diseñen planes de resiliencia cibernética desde los órganos de gobierno de las instituciones, quienes tienen autoridad suficiente para exigir y planificar la implementación de los principios de resiliencia cibernética avanzada, pues son los órganos de gobierno quienes asumen legal, financiera y económica las pérdidas generadas por la vulneración de sus sistemas de información a más de perder credibilidad ante terceros afectando a su reputación.

BIBLIOGRAFÍA

Bazán, Víctor. "El hábeas data, su autonomía respecto del amparo y la tutela del derecho fundamental a la autodeterminación normativa". *Anuario de Derecho constitucional latinoamericano*, No. 37 (2012).

Fernández, Horacio. *Manual de Derecho informático*. Buenos Aires: FEDYE, 2014.

Goche, Mathew, y William Gouveia. *Why cyber security is not enough: you need cyber resilience*. Disponible en ‹https://www.forbes.com/sites/sungardas/2014/01/15/why-cyber-security-is-not-enough-you-need-cyber-resilience/#637818641bc4›.

Gonzales Hoch, Francisco. "Privacidad de la información digital: autodeterminación *vs.* Commodity". *Revista Jurídica de la Universidad de Palermo*, No. 7 (2010).

Hernández, Juan Carlos. "La protección de datos personales en internet y el hábeas data". *Revista Derecho y Tecnología*, No. 13 (2012).

Reyes, Patricia. *Ciudadanas 2020*. Santiago de Chile: Instituto Chileno de Derecho y Tecnologías, 2011.

Soto, Lisa, y Aron Simpson. *Data Protection & privacy 2015 in United States*. Reino Unido: Law Business Research, 2015.

World Economic Forum. *Foundation Statutes.* Reforma al 2006.

World Economic Forum, Boston Consulting Group y Hewlett Packard Enterprise, colaboradores. *Advancing cyber resilience principles and tools for boards*. Ginebra: World Economic Forum, 2017.

Otros

Comisión Interamericana de Derechos Humanos. *El derecho al acceso a la información en el marco latinoamericano.* OEA Ser.L/V/II CIDH/RELE/INF.9/12, 2012.

Comisión Internacional de Electrotecnologías.

Comité Jurídico Interamericano de la OEA. *Principios sobre el acceso al derecho a la información.* OEA, 2008.

Data Protection Act 1998. Reino Unido: The Statutory Office, 1998. Disponible ‹http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf›.

España. *Ley Orgánica 15/1999 de España sobre Protección de Datos de Carácter Personal. BOE*, No. 298, 14 de diciembre de 1999. Disponible en ‹https://www.boe.es/diario_boe/txt.php?id=BOE-A-1999-23750›.

ISO/IEC 27000. Disponible en ‹https://www.iso.org/obp/ui/#iso:std:66435›.

ISO/ICE 27001, 2013. Disponible en ‹https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1›.

Ley Estatutaria 1581 DE 2012 (octubre 17). Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Disponible en ‹http://www.ccomerciotunja.org.co/ccomercio//archivos/rnbd/ley_1581.pdf›.

Organización Internacional de Normalización. Disponible en ‹http://www.iso.org/iso/home/about/the_iso_story.htm›.

Sentencia del Tribunal Constitucional Chileno, Rol No. 1842, 12 de julio de 2011.

Sentencia Evans *vs.* Reino Unido Tribunal Europeo de Derechos Humanos de 2006.

Fecha de recepción: 1 de marzo de 2017
Fecha de aprobación: 28 de abril de 2017

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa

*Andrea Villalba Fiallos**

RESUMEN

La investigación tiene por objeto establecer consideraciones jurídicas sobre el derecho a la intimidad y su vínculo con la protección de datos, para llegar a determinar la importancia de constituir políticas públicas y acciones legislativas que generen un equilibrio ponderativo de derechos y una consolidación de elementos básicos de protección de la información. El análisis inicia con una introducción breve respecto al derecho a la intimidad y aquellos derechos relacionados a ella, para posteriormente tratar el supuesto carácter absoluto del derecho fundamental de la intimidad, y proceder a analizar los elementos constitutivos de dicho derecho, haciendo énfasis en la etapa de *transferencia* de información que tiene que ver con el control y la consecuente entrega de datos a un tercero. Finalmente, el análisis se centra en el estudio de la relevancia de la *autorización* o *consentimiento válido*, y en determinar el nexo causal de la violación del derecho a la protección de datos personales en el derecho a la intimidad por las nuevas tecnologías.

Palabras clave: intimidad, derechos fundamentales, derecho a la intimidad, dato personal, autodeterminación informativa.

ABSTRACT

The investigation has the objective to establish the legal aspects regarding the right to privacy and its connection with data protection, in order to determine the importance of building public policies and legislative actions that can generate a ponderous balance of rights and a consolidation of basic elements of data protection. The analysis begins with a brief introduction regarding the right to privacy and other related rights, and afterwards attends the supposed absolute character of the fundamental right to privacy. In the next part, the constitutive elements will be developed, making emphasis on the phase of *transference* of information established in regard to the control of information and delivered to a third party. Finally, the analysis focuses in the study of the relevance of the *authorization* or *valid con-*

* Abogada patrocinadora del Ministerio de Educación, Ecuador.

sent, and in determining the link to the violation of the right to personal data protection and the consequent infringement of personal data by new technologies.

KEYWORDS: Privacy, Fundamental Rights, Right to privacy, Personal Data, Informative self-determination.

BREVE INTRODUCCIÓN SOBRE EL DERECHO A LA INTIMIDAD Y DERECHOS SUSTANTIVOS RELACIONADOS

Antes de considerar cuestiones específicas relativas al derecho a la intimidad y su vínculo con la protección de datos, es necesario aproximarse al campo de los diferentes derechos que conforman el patrimonio moral de las personas, y que por su naturaleza se encuentran relacionados con el derecho a la intimidad.

Es preciso determinar que el reconocimiento del derecho a la autodeterminación de un individuo es el rasgo característico de una sociedad desarrollada e influenciada diametralmente por los elementos constitutivos de su propio entorno, con influencias de su ambiente de desarrollo tanto antropológicas, políticas como culturales, que facilitan la capacidad de autodeterminarse a sí misma. Esta autodeterminación toma como base conceptos principalísimos, cuyo carácter de primer orden nos hacen clasificarlos a simple vista como derechos inherentes al ser humano.

Este desarrollo social genera un progreso concomitante del Derecho, reconociendo la tutela al honor, al buen nombre, a la intimidad personal y familiar, e incluso a la propia imagen y la voz del individuo, que se constituyen como derechos que si bien es cierto poseen rasgos comunes, finalmente sus aspectos diversos permiten distinguirlos a su vez como derechos diferenciados. En definitiva, podemos catalogarlos como derechos autónomos, estrechamente vinculados entre sí, en tanto que derechos de la personalidad y derivados de la dignidad humana, dirigidos a la protección del patrimonio moral de las personas y al consiguiente resguardo de su información.

Actualmente, el nivel de protección establece una clara evolución a nivel jurídico normativo en lo que se refiere al reconocimiento de derechos, elevados al carácter de fundamentales con el fin de amparar los derechos innatos de los ciudadanos, sin exclusión de ningún tipo.

Es notable, entonces, la influencia que han ejercido los diferentes instrumentos internacionales, que son tomados como base a nivel latinoamericano y por supuesto a nivel legislativo interno ecuatoriano, cuya vertiente desemboca en la aplicación de

características neoconstitucionalistas, cuya particularidad esencial es la primacía de la Constitución y su distinción destacada entre normas jerárquicamente inferiores, dotando de supremacía jurídica a los derechos consagrados en ella, convirtiendo al garantismo en parte fundamental del ejercicio del Derecho y del propio Estado.

Este reconocimiento fehaciente de derechos fundamentales conlleva la premisa de que "el Estado no se justifica a sí mismo",[1] consolidando la visión de un Estado democrático, incluyendo la legitimación del soberano, el sometimiento del *poder* al derecho, y por supuesto el reconocimiento literal plasmado en el Derecho positivo de nuestros derechos subjetivos, objetivos, y finalmente de nuestros derechos fundamentales que por su propia naturaleza "requieren de una serie de pautas hermenéuticas distintas a las que se pueden aplicar al resto de las normas jurídicas"[2] por su correspondiente inherencia humana.

Luigi Ferrajoli, en su obra *Derechos y garantías*, determina una definición formal del concepto de derechos fundamentales y derechos subjetivos, manifestando que:

> son fundamentales los derechos "que no se pueden comprar ni vender", esto es, aquellos derechos subjetivos que corresponden universalmente a "todos" los seres humanos en cuanto dotados del status de personas, de ciudadanos o de sujetos con capacidad de obrar. Por su parte, son "derechos subjetivos" todas las expectativas positivas (de prestaciones) o negativas (de no sufrir lesiones) adscritas a un sujeto por una norma jurídica y en razón de su status o condición de tal, prevista asimismo por una norma jurídica positiva, "como presupuesto de su idoneidad para ser titular de situaciones jurídicas y/o autor de los actos que son ejercicio de estas".[3]

De lo anterior se debe inferir que la persona humana tiene en razón de su ser y de su esencia cosas intrínsecas suyas que reflejan la intimidad, singularidad e irrepetibilidad; así tenemos una definición más clara de derechos fundamentales como aquellos "derechos que están adscritos universalmente a todos en cuanto personas, o en cuanto ciudadanos o personas con capacidad de obrar, y que son por tanto indisponibles e inalienables".[4] Estos elementos contrastados con la definición de derechos naturales constituyen bienes jurídicos adquiridos en razón de la propia naturaleza humana y deben ser respetadas por todos debido a su inherente definición, entonces cualquier lesión de dicho derecho es una ofensa a una realidad personal determinada.

---

1. Gustavo Jalkh Röbens, *Neoconstitucionalismo y Sociedad*. Serie Justicia y Derechos Humanos (Quito: Ministerio de Justicia y Derechos Humanos, 2008), 9.
2. José García Falconí, "Neoconstitucionalismo", *Derecho Ecuador, Revista Judicial*, No. 1 (2014): 1.
3. Luigi Ferrajoli, *Derechos y garantías. La ley del más débil* (Madrid: Trotta, 2004), 37.
4. Miguel Carbonell, *Teoría del neoconstitucionalismo* (Madrid: Trotta, 2007), 71.

El Estado debe garantizar el derecho a la vida privada, y para el efecto se debe recordar aquellos contextos anteriormente utilizados respecto al tema, en los cuales se afirmó que se debe garantizar "el derecho a que lo dejen a uno tranquilo". Es necesario entonces definir a la intimidad como aquel "sinónimo de conciencia, de vida interior",[5] o como el acervo interno de una persona resguardado en su propia psiquis; mientras que el derecho a la intimidad "tiene a proteger al hombre en su aislamiento fecundo y esencial, frente a su semejante, frente a la prensa, frente al Estado".[6]

Al respecto, se debe determinar que el derecho a la intimidad es sin lugar a dudas un elemento esencial de la libertad personal constituido por el derecho a la protección de datos que corresponde a una parte de esa ejecución plena de las libertades otorgadas. Conviene conceptualizar al dato personal como aquel término "utilizado para designar cualquier información relativa a un sujeto identificable",[7] y el derecho a la protección de datos como aquella tutela de la información de carácter personal que incluye su acceso, control y difusión de la misma.

De lo anterior se debe resaltar entonces las garantías que conlleva el reconocimiento de los derechos de carácter personal actualmente elevados al carácter de fundamentales por tutelar la facultad del ser humano a impedir la intromisión no autorizada de los funcionarios públicos o de otros individuos respecto de aspectos o datos personales, en su correspondencia o en sus pensamientos, su hogar, sus comunicaciones, o incluso su tiempo libre.

Recapitulando, es necesario enfatizar en que los derechos fundamentales no son otorgados por los mandamientos constitucionales, que, si bien es cierto los reconocen, su fin trascendental es generar su protección a través de las garantías individuales; sin embargo, este nivel de reconocimiento de derechos le corresponde en definitiva al Estado a través de la desconcentración de sus poderes y dotando de independencia a sus funciones, que, en ejercicio de un estatus democrático, colmado de derechos, otorgará a sus ciudadanos mayor seguridad, reafirmando entonces el principio de seguridad jurídica, desagregando no solo la confianza en la administración de justicia, sino también en las normas emitidas por los legisladores.

---

5. Delia Matilde Ferreira, *El derecho a la intimidad* (Bueno Aires: Editorial Universidad, 1982), 37.
6. Ibíd., 33.
7. Ángeles Gutiérrez Zarza, *Nuevas tecnologías, protección de datos personales y proceso penal* (Madrid: La Ley, 2012), 51.

EL CARÁCTER ABSOLUTO DEL DERECHO FUNDAMENTAL A LA INTIMIDAD

La intimidad como derecho fundamental protege la esfera más privada del individuo, dotada de caracteres reservados que pueden o no compartirse mediante autorización, así encontramos el derecho a la intimidad, con intentos de conceptualizaciones subjetivas, unas más acertadas que otras.

Etimológicamente, intimidad proviene del latín "intimus" superlativo de *interior* y significa "lo que está más adentro, lo más interior, el fondo", el constitucionalista argentino Quiroga Lavié conceptualiza la intimidad como "el respeto a la personalidad humana, del aislamiento del hombre, de lo íntimo de cada uno, de la vida privada, de la persona física, innata, inherente y necesaria para desarrollar su vida sin entorpecimientos, perturbaciones y publicidades indeseadas".[8]

En diferentes fuentes doctrinales, se utiliza de manera indiferente los términos *intimidad* y *privacidad*, sin dotarles de diferencia alguna como si se trataran de dos términos que tienen igual significado, pero dentro de las fundamentaciones más acertadas se debería considerar que responden a concepciones y alcances complementarios, más no diferentes.

El tratadista Germán Bidart Campos se refiere a la intimidad y a la privacidad, de la siguiente manera: "la intimidad es la esfera personal que está exenta del conocimiento generalizado de tercero... y la privacidad es la posibilidad irrestricta de realizar acciones privadas (que no dañen a otros) que se cumplan a la vista de los demás y que sean conocidas por estos".[9]

Evidenciada la diferencia entre la intimidad y la privacidad, se puede colegir que estos son dos conceptos que, analizados bajo criterios únicamente de semántica, se podrían entender como sinónimos, cuya trascendencia a nivel universal genera una asimilación del derecho en demanda de su protección, ocasionando que su vulneración involucre una clara intromisión personal. En lo que respecta a la protección de los mismos, se debe tomar en cuenta que la intimidad al ser considerada como un bien jurídico protegido, y más aún un derecho fundamental mantiene una gama de protección singularizada y complementaria con la privacidad.

---

8. Humberto Quiroga Lavié, *Derecho a la intimidad y objeción de conciencia* (Bogotá: Universidad Externado de Colombia, 1995), 10.
9. Germán Bidart y Walter Carnota, *Derecho constitucional comparado* (Buenos Aires: Ediar, 1998), 137.

Por su parte, la privacidad presenta un alcance que se entiende compatible con la intimidad, sin llegar a la premisa de que son diferentes, hasta el punto de generar como conclusión un silogismo de premisas mayores y menores: "los asuntos íntimos son privados, pero no todos los asuntos privados pueden tener carácter de íntimos". Es decir, cuando se vulnera la intimidad, que engloba áreas muy concretas de la vida de una persona, se ha vulnerado a la vez a la privacidad o aspectos generales referentes a una persona; pero cuando se ha vulnerado la privacidad, no necesariamente significa que se ha atentado contra la intimidad sin perjuicio de que efectivamente pueda llegar a producirse.

Retrotrayendo el análisis a los antecedentes puntuales de la intimidad, se conoce que esta tiene sus primeros pasos de carácter social y posteriormente jurídico con el conocido artículo "The Right of Privacy" (El derecho a la privacidad), de Luis Brandeis y Samuel Warren, constituida como uno de los ensayos más influyentes en la historia de la legislación estadounidense, pues por primera vez nació el concepto de la intimidad como un derecho, y por tanto un bien jurídico tutelable y de propiedad inherente a las personas, cuya importancia generó el estudio y aplicación de medidas para que este sea debidamente protegido.

El derecho a la intimidad personal se encuentra protegido constitucionalmente, e incluso se podría considerar que esta tutela del derecho es irrenunciable, inalienable e imprescriptible por la naturaleza jurídica que contiene; por tanto, la renuncia a este derecho es inconsistente. Sin embargo, es esencial recordar que este derecho como tal no es de carácter absoluto; lo mismo sucede con la protección de datos: estas son prerrogativas que deben ejercerse dentro de límites razonablemente impuestos en consonancia de los derechos de los demás.

Partiendo de la premisa, y tomando en cuenta que el derecho a la intimidad se vincula a la esfera más reservada de las personas, es decir, al ámbito que constituye un secreto para los demás y que se aleja totalmente del conocimiento público, ámbito aquel que el propio individuo desea mantener oculto a los demás por pertenecer a su esfera más privada,[10] que además se encuentra vinculado con la dignidad y el libre desarrollo de la personalidad. Es por tanto un derecho innato de las personas sin importar proveniencia, nacionalidad o autodeterminación, ya que de esta forma el derecho a un núcleo inaccesible de intimidad se reconoce incluso a las personas más expuestas al público.

---

10. Sentencia Tribunal Constitucional Español No. 151/1997, del 29 de septiembre de 1997.

La intimidad, de acuerdo con el precepto constitucional, no solo se reconoce al individuo aisladamente considerado, sino también al núcleo familiar,[11] y además ahora se encuentra constitucionalizado el derecho a la protección de los datos de carácter personal que garantiza a los individuos un poder de disposición y control sobre ellos.

En líneas anteriores se determinó que el derecho a la intimidad no es absoluto y, por tanto, en determinadas ocasiones justificadas cederá frente a otros bienes jurídicamente protegidos, quizá en aquellos en los que se establezca la necesidad, bajo la siguiente premisa consciente: "siempre que esté justificado y resulte proporcional, sobre la base de otros derechos u otros bienes jurídicamente protegidos de interés general".

Al considerar a la intimidad como un derecho de carácter no absoluto, y por lo tanto confirmando su carácter relativo, la protección de información se condiciona a ciertas circunstancias y se justifica la posibilidad de vulnerarla en diversas expresiones ya sea ante exigencias públicas y/o judiciales que se encuentran subyugadas a ciertos parámetros, así lo expresa Michel Foucault cuando dice: "y si le es preciso todavía a la justicia manipular y llegar al cuerpo de los justiciables, será de lejos, limpiamente, según unas reglas austeras, y tendiendo a un objetivo mucho más "elevado";[12] sin embargo, es preciso observar que la Constitución no ha establecido de modo expreso la reserva de intervención judicial. Sin embargo, otras normas de carácter penal sí determinan la existencia de dicha reserva judicial, como en el propio allanamiento de morada, que no solo violenta el domicilio, sino a su vez a la intimidad personal y familiar, pero que debidamente justificado en el ejercicio del deber procesal ameritan ciertas acciones invasivas.

Respecto de lo anterior se puede colegir que la legitimación de la vulneración de la protección de datos, y a su vez de la afectación de la intimidad, se encuentra en el carácter oficial de la solicitud; es decir, su injerencia solo puede ser posible mediante decisión judicial debidamente motivada, que también tiene como fin prever que su ejecución sea respetuosa de la dignidad de la persona y no constituya violación a otro tipo de derechos inherentes al ser humano.

Sin embargo, la afirmación de ese interés público para justificar el sacrificio del derecho a la intimidad, y por lo tanto a la entrega de datos, no es suficiente para que la garantía constitucional de este pierda concreción; por lo tanto, no es solo la regularidad formal de la decisión judicial que motive el hecho de acuerdo al marco jurídico normativo vigente, sino también la sana crítica y razonamiento de la autoridad actuan-

---

11. Sentencia del Tribunal Constitucional Español No. 197/1991, 17 de octubre de 1991.
12. Michel Foucault, *Vigilar y castigar: nacimiento de la prisión* (Buenos Aires: Editorial Argentina, 2002), 13.

te, ya sea en el ámbito judicial o administrativo claramente vinculados al revestimiento de la atribución de limitar el derecho a la intimidad.

Por lo tanto, debe presentarse una necesidad absoluta respecto de la toma de esa decisión, considerando la concurrencia de una situación específica que genere de forma intrínseca la justificación de la limitación de derechos y principalmente de establecer la estimación de proporcionalidad de los bienes jurídicos y la situación en que se halla aquel individuo a quien se la impone.

Habrá entonces que ponderar siempre el interés público para justificar el sacrificio del derecho a la intimidad, integridad física *versus* las garantías constitucionales que perdería el individuo a cambio de la posible obtención de indicios probatorios que pueden llegar incluso al esclarecimiento de situaciones jurídicas obscuras, sosteniendo que no se pueda llegar a la verdad material de otro modo.

Lo trascendental en este punto es corroborar si el administrador de justicia logrará alcanzar una justificación constitucional objetiva y razonable de las cuestiones que le han llevado a ejecutar esta medida de intromisión de la intimidad, o si, por el contrario, habiendo sido revestido de juez le corresponde la obligación de encontrar cualquier otra medida que permita no producir menoscabo de derechos fundamentales.

A tal efecto conviene definir los requisitos que conformarían de forma idónea el análisis sobre la proporcionalidad, al respecto de los cuales pueden resumirse en: 1. que la medida limitativa del derecho fundamental esté prevista por la Ley; 2. que la medida sea adoptada mediante resolución judicial especialmente motivada; y 3. que la medida sea idónea, necesaria y proporcional en relación con un fin constitucionalmente legítimo.

Hay que mencionar además que los derechos reconocidos en la Constitución en el art. 66 podrán verse afectados ya sea de manera independiente, pero también y con frecuencia de forma conjunta, dada su evidente proximidad estos derechos tienen su más inmediato riesgo en el ejercicio de las libertades de expresión e información, lo que llevará a que la aplicación de la ponderación de bienes jurídicos constituyan un ejercicio habitual por parte de los operadores y administradores del derecho.

ELEMENTOS DE ANÁLISIS DE LA INTIMIDAD EN LA PROTECCIÓN DE DATOS

El derecho a la intimidad debe ser examinado desde ciertas ópticas (territoriales, temporales e individuales) que permitan definir de mejor manera su ámbito de acción para generar premisas que coadyuven a la valoración de su alcance y aplicación.

Partiendo de la premisa kantiana que considera al hombre, como un "ser" dotado de razón y concebido por lo tanto con la capacidad de conocer su libertad para plasmarla en su independencia y autonomía, generando el ejercicio de su propia naturaleza en cada momento, sin excluir elementos temporales, territoriales o espaciales.

Elemento territorial

Entendiendo al territorio como aquella extensión de la superficie terrestre, se configura la convicción de que no se puede limitar el derecho a la intimidad a ciertos espacios, o lugares, genéricamente denominados como "privados" y/o "íntimos", ya que es insostenible mantener la afirmación de que en los espacios públicos, abiertos o al aire libre no ejercemos nuestra propia autodeterminación, nuestras entrañadas facultades e inherentes prerrogativas. Tal es así que es poco más que inexacto afirmar que, de acuerdo al lugar, no podríamos actuar como lo que somos "seres humanos" y desarrollar actividades privadas, que por tal carácter el titular del derecho prefiere mantenerlas únicamente bajo su conocimiento sin existir por lo tanto autorización de divulgación alguna.

No cabe duda de que el derecho a la intimidad se encuentra extendido hasta cualquier lugar en el que se encuentre el titular, por lo tanto no reducido a su localización, sino por el contrario dotando de irrelevancia el ámbito físico en el que el titular se encuentre y haciendo énfasis en la esencia propia de lo que significa la inherencia de un derecho fundamental.

Hay premisas que fundamentan el ámbito territorial del derecho a la intimidad con la convicción de que no puede considerarse privado bajo ninguna circunstancia lo que se realiza a la vista de todos; sin embargo, cabe aclarar que esta concepción poco progresista posee en su haber un carácter inconstitucional, ya que pretende destruir el sentido de la intimidad como derecho fundamental, y, por lo tanto, lo desvincula de la dignidad humana. Tal es el caso que algunos autores, al referirse al derecho a la intimidad tanto personal como familiar, han determinado que tales derechos son derechos originarios e innatos, absolutos, extrapatrimoniales, irrenunciables, inembargables e inexpropiables y son imprescriptibles.

Elemento temporal

En este punto es imprescindible referirnos a los planteamientos aristotélicos concernientes al tiempo ya que "solo cuando percibimos un antes y un después hablamos de tiempo, porque el tiempo es justamente esto, dice Aristóteles, número del movi-

miento según el antes y el después".[13] Habrá entonces que clasificar dos momentos cruciales para poder analizar la temporalidad del derecho a la intimidad y la protección de datos; el primero concerniente a la permanencia vital del individuo ligada al movimiento; y el segundo concerniente a su muerte o etapa *post morten*.

Como se pudo apreciar en reflexiones anteriores, es innegable la cobertura del derecho a la intimidad durante la vida de un individuo, de tal modo que se reconoce su estatus de derecho fundamental, vinculado entonces a la mera existencia del sujeto y considerándolo como un elemento innato de las personas, entendido esto nos queda tratar entonces la cuestión de ¿qué sucede con la personalidad pretérita?

Para responder esa pregunta debemos partir de la base de que con la muerte se extingue la persona y con ella la personalidad jurídica, tal como lo establece el art. 64 del Código Civil ecuatoriano. Con esta premisa entonces debería entenderse que la "persona" termina con la muerte.

De lo anterior nace la duda de si existe "tutela post mortem" respecto del derecho a la intimidad y la protección de datos. Al respecto debemos tomar en cuenta que los derechos promulgados en la Constitución se encuentran plasmados bajo el reconocimiento y garantía de derechos a las "personas"; por lo tanto, si el estado de "persona" termina con la muerte, entonces no se podría reconocer la tutela de derechos de la personalidad pretérita en el marco jurídico ecuatoriano, constatando un vacío legal que amerita ser tratada a nivel legislativo, para cubrir necesidades prácticas para resolver las diferentes situaciones que se pueden producir por intromisiones en la *memoria defuncti*.[14]

Al respecto, se deberá regular entonces aspectos relacionados directamente con la herencia no patrimonial del causante y el traslado de la titularidad del derecho a sus causahabientes, para delimitar la amplitud y alcance de su ejercicio, con el objeto de precautelar la trascendencia de la existencia de la persona debiendo por lo tanto proteger su memoria y el recuerdo que predomina de ella, prolongando la personalidad extinguida por la muerte mediante el otorgamiento de la nueva titularidad del derecho a los herederos.

---

13. Alfonso Pérez, *Tiempo e historia: una filosofía del cuerpo* (Madrid: Encuentro, 2002), 269.
14. María Cobas Cobiella, "Protección post mortem de los derechos de la personalidad. Reflexionando sobre la cuestión", *Revista Boliviana de Derecho*, No. 15 (2013): 112-29.

Elemento individual o subjetivo

Es imperativo delimitar como puntualización concreta que la extensión del derecho se ve condicionada por ciertas circunstancias referentes a la persona como tal, o el aspecto concreto de su vida que se ve afectado.

De acuerdo a las circunstancias particulares del individuo y del caso, es importante mencionar que en ocasiones se ha interpretado que el alcance de la intimidad viene determinado por el propio afectado, no obstante, es necesario aclarar que el alcance del derecho a la intimidad no acapara únicamente el ámbito de la información. Así las injerencias a la intimidad no solo provienen de excesos en las libertades de expresión o información, al contrario, la protección del derecho se muestra imprescindible también en ámbitos como el de uso de información de instituciones públicas, y uso de bases de datos, refiriéndose entonces a aquel control idóneo, necesario y equilibrado del uso de los datos otorgados al Estado, o de aquellos que supongan una injerencia en la intimidad de los ciudadanos afectados injustificada o desproporcionadamente.

TRANSFERENCIA DE DATOS E INFORMACIÓN

Dicho lo anterior es necesario referirse a la *transferencia* como causa ineludible de la titularidad del derecho a la intimidad y el innato poder de control de datos, con el fin de determinar con facilidad la posible vulneración de derechos personales en la actual evolución tecnológica, vinculando el análisis a la expresión de la voluntad del titular con la existencia de la *autorización* y complementándolo respecto.

El avance de la sociedad conjuntamente con el desarrollo tecnológico va generando la aparición de nuevos riesgos a la intimidad, desde el llamado "right to be let alone" aplicado en la jurisprudencia estadounidense hasta llegar al día de hoy, en el que el propietario o titular del derecho confiere o transfiere el poder y control de su información y/o de sus datos, plasmándolo quizá en la premisa exagerada de dotar a otro el poder de uno mismo y de su propia información.

Esta *transferencia* genera una visión de protección alterada y hasta de carácter indirecto de un derecho constituido como innato y fundamental. Observando este comportamiento desde un punto de vista magnificado si relacionamos este análisis con la teoría penal sobre la causalidad, entendiendo aquella realidad fáctica según la cual se entrega el poder de control de nuestra información a un tercero y entendiendo que a toda causa le sigue un resultado final, el nexo unificador es la llamada "relación de causalidad", entre la forma de la entrega de información y la supuesta lesión del derecho.

En este sentido, el análisis jurídico correcto para determinar la violación del derecho a la intimidad a nivel general, tanto dentro del ámbito público como privado, subyace en la determinación de aquella ausencia de un *consentimiento válido* para acceder a la información o del consentimiento para utilizarla de manera específica, en tanto y en cuanto la acción relevante será la forma de obtención de dicha información, debiendo determinar si esta fue entregada de forma legítima (autorización) y sin embargo fue utilizada para un fin distinto para el que fue otorgada, o no; o si simplemente la ausencia de la respectiva autorización es latente, partiendo de esta base podemos enfocarnos en la existencia de la posible lesión del derecho a la intimidad.

Tomando en cuenta el número 11, art. 66 de la Constitución del Ecuador, que protege de manera general los elementos más arraigados al "ser humano", así como el *modus* de utilización de la información personal reflejada y vinculada a una autorización del titular, en concordancia con el número 19 de la misma norma, que determina lo que en líneas anteriores ha sido definida como *transferencia*, garantizando del siguiente modo esta interacción personal:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y a la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución y difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Esta norma supedita como elemento indispensable dicha autorización de uso, al tácito *negocio jurídico* constituido por la voluntad de las partes para generar o producir un determinado efecto; por lo tanto, si el efecto ocasionado es diverso al que se convino, se debería determinar el límite y los efectos que generaría circunscrita autorización, llegando a determinar el exceso de la atribución otorgada, tanto a nivel privado con un individuo de la sociedad civil como en el sector público; lo que nos lleva a determinar que el consentimiento debe ser expreso o tácito, pero siempre inequívoco, ya que de corroborar el consentimiento del titular este se torna en causal de justificación.

Habiendo entonces analizado la información y la consecuente autorización en un contexto más privado, es necesario abordar lo que respecta al papel del Estado en la tutela de derechos y su capacidad de injerencia en la intimidad de sus ciudadanos: es indispensable referirse a la Sentencia de la Corte Interamericana de Derechos Humanos del Caso Artavia Murillo y otros *vs.* Costa Rica, sobre la "fecundación in vitro" del 28 de noviembre de 2012,[15] caso en el cual se puede evidenciar el exceso de poder

15. Sentencia de la Corte Interamericana de Derechos Humanos, Caso Artavia Murillo y otros ("fecundación in vitro") *vs.* Costa Rica, 28 de noviembre de 2012.

en el uso de las prerrogativas exorbitantes del Estado y el alto nivel de intromisión y vulneración al legalizar la prohibición de métodos artificiales de concepción (fecundación in vitro), generando circunstancias inconcebibles que se pueden producir por el hecho de no reconocer derechos naturales, fundamentales e innatos, amparados en justificaciones no proporcionales respecto del bien jurídico a proteger y el bien jurídico finalmente perjudicado.

Es evidente la intervención invasiva del derecho a la autodeterminación individual que recae sobre la libre elección de procreación, ya sea mediante el uso de medidas directas o bajo el uso de mecanismos artificiales, vulneración que engloba la autonomía personal y libertad de llegar a ser progenitor y todas aquellas decisiones que engloban la esfera más íntima de la vida privada y familiar del ser humano y que forman parte del ejercicio de las libertades personales universalmente reconocidas.

En este caso, la dignidad humana fue objeto de constantes violaciones, incluso a nivel mediático, ya que se divulgó variada publicidad de carácter discriminatorio y estigmatizante en contra de la situación de desventaja de los accionantes, evidenciando su estado de incapacidad de concebir, y emitiendo juicios de valor respecto de la infertilidad, provocando daños en los derechos personales y en el patrimonio moral de los accionantes a causa del linchamiento mediático constituido.

La violación referida se evidencia en la clara exposición de información privada en los medios de comunicación, en ausencia del elemento que prevendría la configuración de un delito, y se constituye como la expresión volitiva que demuestre un consentimiento expreso de la divulgación de información (autorización), generando daños morales.

Es inaudito conservar por casi once años una política prohibitiva, intrusiva y discriminatoria, claramente constituida en restricción desproporcionada de derechos y libertades, que, aprovechando el carácter relativo del derecho a la intimidad y en uso de las atribuciones estatales, pretendió legalizar y legitimar una vulneración de derechos individuales sin siquiera aplicar el principio de proporcionalidad y los elementos necesarios para habilitar actuaciones limitativas de derechos, que, como se determinó en líneas anteriores, deben confluir ciertos elementos que son necesarios para justificar el quebrantamiento de dicho derecho; en tal razón y por varias consideraciones relacionadas, la Corte confirmó que la privacidad se caracteriza por quedar inmune a las invasiones o lesiones abusivas o arbitrarias por parte de terceros o de la propia autoridad pública.

Dicho lo anterior, es necesario mantener un análisis respecto de la información consolidada a nivel público, ya sea dentro de bases datos, ficheros y/o información generada o incluida en sistemas electrónicos. Cabe recalcar que como "civitas" y en ejercicio de nuestro estatus generamos información pública y privada que se va consolidando en las diferentes instituciones del mismo carácter; dicha información se

encuentra protegida de su ilegal revelación elevando este acto a delito, y por lo tanto conformando la integración de un bien jurídico en el art. 229 del Código Orgánico Integral Penal (COIP), previniendo la protección de los datos íntimos y personales haciendo alusión al carácter esencialmente valorativo del derecho penal cuyo fin último presupone la protección de los bienes jurídicos.

En Ecuador se ha promulgado la Ley del Sistema Nacional de Registro de Datos Públicos,[16] que a su vez crea la llamada Dirección Nacional de Registro de Datos Públicos (DINARDAP), a la que se le atribuye facultades de ejecución de procesos y regulación del sistema de registro de datos públicos y su acceso, asumiendo la consolidación estandarización y administración de una base de datos única de todos los Registros Públicos, para generar un sistema de interconexión, también llamado de "control cruzado" de la información de los ciudadanos.

De lo anterior nace la duda de ¿hasta qué punto es procedente y positivo un enlace y conexión de toda la información ciudadana en un solo órgano? Considerando que ello supone la concurrencia de dos elementos esenciales: el primero es la existencia de un determinado estándar normativo de conocimiento tanto del agente controlador, como del individuo que es objeto de dicho control o actividad; y el segundo es la formulación por la "autoridad" o "agente de control" de un juicio o premisa adecuado respecto del carácter informativo a vincular,[17] con el objeto de salvaguardar la seguridad jurídica correspondiente en la conexión de datos, previniendo que las actuaciones administrativas no excedan de sus facultades.

Una vez que el titular transfiere la información al Estado y este la obtiene se configura un vínculo entre ambos, en el cual el Estado tiene que garantizar su protección mediante el principio de seguridad y principio de confidencialidad de los datos, resguardando la referida información de manera que no pueda existir ningún riesgo de divulgación.

Es indispensable recalcar que el requisito imprescindible para delimitar si estos derechos han sido o pudieron haber sido violados, se lo consigue bajo el análisis de los actos presuntamente lesivos, y si estos se efectuaron con o sin la correspondiente autorización del sujeto, es decir, con el respectivo consentimiento que cabe mencionar puede ser revocado en cualquier momento. En este sentido, lo óptimo a nivel legislativo sería que se establezca taxativamente en qué casos no se apreciará la existencia

16. Ley del Sistema Nacional de Registro de Datos Públicos promulgada en el Registro Oficial Suplemento No. 162 el 31 de marzo de 2010, y elevada al carácter de orgánica mediante ley publicada en el Registro Oficial Segundo Suplemento No. 838 de 3 de diciembre de 2012.
17. Alberto Cerda, "Mecanismos de control en la protección de datos en Europa", *Revista Ius et Praxis*, No. 12 (2006): 221-51.

de intromisión ilegítima en el ámbito protegido como en el caso de que estuviere expresamente autorizada por ley, o, en su defecto, cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso.

EL DERECHO A LA PROTECCIÓN DE DATOS EN LAS NUEVAS TECNOLOGÍAS

A continuación se analizará cómo el desarrollo de las tecnologías hace indispensable el estudio de la autodeterminación informativa como elemento primordial en la protección de datos, la vida privada y el derecho a la intimidad.

Como nos hemos referido en líneas anteriores, el concepto de intimidad suele ser controversial; sin embargo, tenemos clara la esencia de su definición, a pesar de que incluso el "Comitee on Privacy" británico concluyó la imposibilidad de definir satisfactoriamente el concepto de intimidad, por su carácter subjetivo, general y amplio; por tanto, comprendiéndola simplemente como un derecho fundamental, y relacionándola con las nuevas tecnologías, es obvio pensar que este derecho tiene exorbitantes posibilidades de ser vulnerado y más aún cuando asemejamos al internet con una sociedad que es indudablemente anónima, en la cual el desconocimiento de ciertos usuarios es común pero en el cual la información está completamente digitalizada y se corre el riesgo permanente de que la información y los datos pueda ser ilegalmente obtenidos y difundidos, ya que los datos de un individuo quedan públicamente expuestos en el ciberespacio.

En este punto, debemos determinar que la Constitución no solo tiene como objeto la protección de la vida de la persona frente a cualquier tipo de invasión, tomando en cuenta que el individuo desea excluir del conocimiento público y de las intromisiones de terceros, información que un sujeto la determina como suya y personal, por lo tanto es el derecho a la protección de datos el que "tiene como objeto garantizar a esa persona un 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 afectado".[18]

De lo anterior, el derecho a la intimidad le permite al individuo excluir cierta información del conocimiento público, y resguardar sus datos personales de una publicidad no voluntaria, y el derecho a la protección de datos reconoce al individuo la facultad de controlar sus datos personales y a su vez la capacidad de disponer y decidir sobre los mismos. Tal es así que el derecho a la protección de datos garantiza al ciudadano

18. Abel Téllez Aguilera, *Nuevas tecnologías. Intimidad y protección de datos* (Madrid: Edisafer, 2001), 73.

la forma de uso de estos, es decir, el individuo tiene poder de disposición sobre los mismos, a esta facultad hay que agregarle la posible dificultad del ejercicio de este poder con el hecho de desconocer qué datos se encuentran en posesión de terceros, quienes los poseen y con qué finalidad.

Así lo determina el tratadista Oscar Puccinelli, citado en la Sentencia 001-14-PJO-CC de la Corte Constitucional del Ecuador,[19] refiriéndose al respecto como:

> El derecho a la protección de datos –y específicamente, su elemento denominado "autodeterminación informativa"–, tiene un carácter instrumental, supeditado a la protección de otros derechos constitucionales que se pueden ver afectados cuando se utilizan datos personales, como puede ser la intimidad, la honra, la integridad psicológica, etc.[20]

En este sentido, el llamado derecho a la protección de datos lleva consigo arraigado un contexto evolucionado, tomando en cuenta que este extiende las garantías del derecho a la intimidad en su dimensión constitucionalmente protegida, y abarca los bienes de la personalidad que se refieren a la vida privada vinculada a cualquier tipo de dato personal en el uso de las nuevas tecnologías, conteniendo en su haber la autodeterminación informativa conceptualizada como "aquella necesidad de que los ciudadanos controlen la información que les concierne, ya no como un mero derecho de defensa frente a las intromisiones de otros, sino ahora, y frente a los riesgos tecnológicos, como un derecho activo de control sobre el flujo de informaciones que circulan sobre nosotros".[21]

La autodeterminación informativa comporta el derecho de toda persona a ejercer control sobre la información personal que le concierne, frente a cualquier ente público o privado. Cabe mencionar que este derecho fue utilizado por primera vez por el Tribunal Constitucional Federal de Alemania, en la sentencia sobre la Ley del Censo del 15 de diciembre de 1983, con la que se faculta a las personas a decidir y consentir de manera informada y libre el uso de sus datos personales por terceros, ante el tratamiento automatizado de los mismos.

Es así que el derecho a la protección de datos personales se deriva del derecho a la vida privada y por lo tanto del derecho a la intimidad, los cuales no dejan de verse amenazados por las nuevas tecnologías que modifican formas de distribución de la información y hasta de almacenamiento; sin embargo, proyectando el uso tecnológico

---

19. Sentencia 001-14-PJO-CC, sentencia de jurisprudencia vinculante presentada en el caso No. 0067-11-JD, *Gaceta Constitucional* No. 007, 3 de julio de 2014, 6.
20. Oscar Puccinelli, *El Habeas Data en Indoiberoamérica* (Bogotá: Temis, 1999), 68.
21. Winfried Hassemer, *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales* (Buenos Aires: Editores del Puerto, 1997), 124.

para plasmarlo en el derecho positivo para llegar al bien común se debe mencionar la necesidad de promulgación de leyes y políticas públicas que establezcan límites a la libertad humana y que generen un equilibrio entre los derechos propios y ajenos, que se establezcan como principios básicos de toda sociedad.

De lo anterior, es claro que la protección de datos y por lo tanto el derecho a la intimidad pueden verse vulnerados por el constante desarrollo de las tecnologías, las redes sociales, los inventos de reproducción de la imagen y la voz: en general, por los diferentes medios de comunicación masivos creados; por lo tanto es así como se genera la necesidad de proteger la información, tomando en cuenta que en 1789 con la Revolución francesa se proclamaron ya en el derecho positivo las garantías para el ejercicio de las libertades.

Sin embargo, con la creación de las nuevas tecnologías, el bien jurídico más susceptible de ser lesionado o puesto en peligro es el derecho a la intimidad, a pesar de que los usuarios de internet pretenden disfrazar su identidad y tutelar de alguna forma sus datos y privacidad por medio del *anonimato* en la comunicación y utilizando como complemento tácito la dificultad de rastrear datos reconocibles.[22]

> es unánime la denuncia de que las nuevas tecnologías suponen un serio peligro para la intimidad, ya que la facilidad con que esta puede verse vulnerada va en aumento, a medida que avanzan, se perfeccionan y simplifican las técnicas de grabación, capacitación de imágenes, reproducción y transmisión de datos.[23]

Tomando en cuenta la necesidad e importancia que tiene actualmente a nivel mundial la tecnología, y más aún el internet en nuestro diario vivir, es difícil comprender cuán complicada es la generación de una regulación clara y unitaria del internet, como expone José de Areilza Carvajal en su artículo denominado "¿Quién gobierna Internet?", estableciendo la paradoja entre la existencia de la sociedad del conocimiento generada por las redes y la carestía de controles adecuados que salvaguarden nuestros datos personales.

Sin embargo, se debe tomar en cuenta que, en un determinado momento del desarrollo de la sociedad, se llegó al llamado período instrumental de internet,[24] en el cual se definió al internet como un espacio abierto a la información de todos y en donde se pueden realizar las más diversas relaciones jurídicas, tomando de esta forma

---

22. Manuel Castells, *La galaxia internet* (Barcelona: Areté, 2001), 193.
23. Concepción Conde Ortiz, *La protección de datos personales* (Madrid: Dykinson, 2005), 20.
24. Ricard Ruiz de Querol, "Más allá de la primera era de internet", *Nueva Revista de Política, Cultura y Arte*, No. 70 (2000): 1.

conciencia de que al existir relaciones jurídicas era necesario establecer elementos vinculantes de carácter normativo y de control para su uso.

A esto debemos referirnos, al derecho al acceso universal a las tecnologías de información y comunicación, tomando como base fundamental el número 2 del art. 16 de la Constitución ecuatoriana, que garantiza la libertad informática y otros derechos ampliamente reconocidos y relacionados. Así tenemos la dignidad humana, la libertad de expresión y por supuesto la libertad de comunicación, etc. En este sentido sí podemos vincular el derecho de libertad informática con otros tantos derechos, de carácter inherente al desarrollo de la personalidad humana; entonces utilizando los principios constitucionales, el apoyo de los derechos ampliamente reconocidos en la norma suprema y los tratados internacionales se resalta y sobresale la necesidad de extender la tutela de derechos que por el continuo desarrollo de la sociedad se convierten en indispensables, como sucede con la tutela del derecho a la libertad informática a nivel universal.

Es cierto que la protección de datos personales en ciertos casos se enfrenta ante ciertos derechos, tal es el caso de la libertad de expresión, o el derecho a la información, constituyéndose como factor necesario que los sistemas constitucionales en amparo de los derechos fundamentales protejan las diferentes libertades individuales y colectivas, amparados en la ponderación de derechos y contrastados en el posible sacrificio de un derecho reducido por uno mayor.

CONCLUSIONES

- La autodeterminación informativa presupone la capacidad de dominio y control del individuo sobre su propia información y respecto del estatus que el titular del derecho le quiere dar a esta, ya sea conservarla dentro de su acervo privado o constituirla como información de conocimiento público.
- La injerencia o violación de la intimidad se determina por el *modus* de transferencia de la información enmarcándola en la presuposición de la existencia de un consentimiento expreso o tácito configurado como *autorización* y la necesaria exteriorización de un *consentimiento válido* que genere la consecuente entrega del poder de control de datos a un tercero.
- La clara ausencia de consentimiento válido podría generar una situación ponderativa de derechos entre la protección de datos personales y la autodeterminación informativa que en casos particulares puede exigir la revelación de determinados elementos pertenecientes a la vida privada de un sujeto, siempre que tal circunstancia sea justificada por motivos en beneficio del interés general.

- El derecho a la intimidad y la protección de datos de la personalidad pretérita deben ser regulados y controlados, para cubrir el vacío legal que existe en Ecuador respecto al ejercicio y aplicación de la herencia del patrimonio moral del *causante* y de sus nuevos titulares, con el objeto de instrumentar y resolver las problemáticas que se pueden producir por vulneraciones a la memoria defuncti.
- El avance tecnológico genera nuevas formas de vulneración de derechos personales, transgrediendo la protección de datos individuales y el bien jurídico fundamental de la intimidad, generando la necesidad latente de la promulgación de normativa y políticas públicas que establezcan límites a ciertas libertades humanas que generen un equilibrio entre los derechos propios y ajenos.

BIBLIOGRAFÍA

Bidart, Germán, y Walter Carnota. *Derecho constitucional comparado*. Buenos Aires: Ediar, 1998.

Carbonell, Miguel. *Teoría del neoconstitucionalismo*. Madrid: Trotta, 2007.

Castells, Manuel. *La Galaxia Internet*. Barcelona: Areté, 2001.

Cerda, Alberto. "Mecanismos de control en la protección de datos en Europa". *Revista Ius et Praxis*, No. 12 (2006).

Cobas, María. "Protección post mortem de los derechos de la personalidad: reflexionando sobre la cuestión". *Revista Boliviana de Derecho*, No. 15 (2013).

Conde Ortiz, Concepción. *La protección de datos personales*. Madrid: Dykinson, 2005.

Falconí, José García. "Neoconstitucionalismo". *Derecho Ecuador, Revista Judicial*, No. 1. 2014.

Ferrajoli, Luigi. *Derechos y garantías. La ley del más débil*. Madrid: Trotta, 2004.

Ferreira, Delia Matilde. *El derecho a la intimidad*. Buenos Aires: Editorial Universidad, 1982.

Foucault, Michel. *Vigilar y castigar: nacimiento de la prisión*. Buenos Aires: Editorial Argentina, 2002.

Gutiérrez Zarza, Ángeles. *Nuevas tecnologías, protección de datos personales y proceso penal*. Madrid: La Ley, 2012.

Hassemer, Winfried. *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales*. Bueno Aires: Editores del Puerto, 1997.

Jalkh Röbens, Gustavo. *Neoconstitucionalismo y sociedad*. Serie Justicia y Derechos Humanos. Quito: Ministerio de Justicia y Derechos Humanos, 2008.

Pérez, Alfonso. *Tiempo e historia: una filosofía del cuerpo*. Madrid: Encuentro Ediciones, 2002.

Puccinelli, Oscar. *El Habeas Data en Indoiberoamérica*. Bogotá: Temis, 1999.

Quiroga Lavié, Humberto. *Derecho a la intimidad y objeción de conciencia*. Bogotá: Universidad Externado de Colombia, 1995.

Ruiz de Querol, Ricard. "Más allá de la primera era de internet". *Nueva Revista de Política, Cultura y Arte*, No. 70 (2000).

Téllez Aguilera, Abel. *Nuevas tecnologías. Intimidad y protección de datos*. Madrid: Edisafer, 2001.

Otros

Sentencia 001-14-PJO-CC, Sentencia de Jurisprudencia vinculante presentada en el Caso No. 0067-11-JD, *Gaceta Constitucional* No. 007, 3 de julio de 2014.

Sentencia de la Corte Interamericana de Derechos Humanos, *Caso Artavia Murillo y otros ("Fecundación in Vitro") vs. Costa Rica*, 28 de noviembre de 2012.

Sentencia del Tribunal Constitucional Español No. 197/1991, 17 de octubre de 1991.

Sentencia Tribunal Constitucional Español No. 151/1997, del 29 de septiembre de 1997.

Fecha de recepción: 15 de marzo de 2017
Fecha de aprobación: 12 de mayo de 2017

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales

*Luis Enríquez Álvarez**

RESUMEN

Ecuador necesita contar de urgencia con una ley de protección de datos personales que regule la manera como las instituciones nacionales y extranjeras tratan, procesan, conservan, y explotan comercialmente los datos personales de las personas naturales en Ecuador. Nuestro país debe cumplir con estándares mínimos, para llegar a ser considerado como un país confiable para la transferencia de datos personales, lo cual permitiría el surgimiento de empresas ecuatorianas transnacionales en internet, con el objeto de que puedan realizar el tratamiento de datos personales de ciudadanos de todo el mundo.

Este artículo tiene la finalidad de analizar las falencias jurídicas del proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales con el fin de corregirlas, y proponer el desarrollo de una ley de protección de datos personales que esté sincronizada con la legislación de otros países, y la realidad técnica de las tecnologías de la información.

Palabras clave: datos personales, privacidad, derechos fundamentales, derecho al olvido, seguridad de datos, confidencialidad, procesamiento de datos.

ABSTRACT

Ecuador urgently needs to create a data protection law to protect the rights of natural persons in relation to the processing, conservation, and explotation of their personal data by public and private institutions. Our country is required to comply with minimum standards in order to be considered as a trusted country for personal data transfers, allowing the emergence of transnational Ecuadorian enterprises treating personal data of foreign citizens from worldwide on Internet.

* Consultor de seguridad informática, y perito en informática forense.

This article aims to analyze some missconceptions of the project named Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales with the purpose of recommend some corrections. Furthermore, this article proposes the creation of a data protection act which is synchronized with other countries laws, and the technical reality of information technologies.

KEYWORDS: personal data, privacy, fundamental rights, right to be forgotten, data security, confidentiality, data processing.

FORO

INTRODUCCIÓN

Las primeras nociones sobre el derecho a la vida privada surgen a finales del siglo XIX.[1] Sin embargo, a partir de la segunda mitad del siglo XX el derecho a la vida privada adquiere mayor relevancia. La *Declaración Universal de Derechos Humanos* de 1948 establece las bases del derecho humano a la vida privada.[2] En las décadas posteriores, el desarrollo de las redes de telecomunicaciones y los sistemas informáticos, conllevaron a la creación de instrumentos jurídicos nacionales y supranacionales para proteger este derecho.

La protección de datos personales surge como un mecanismo jurídico para proteger el derecho a la vida privada de las personas en la era de las tecnologías de la información. Sus objetivos principales son: definir a los *datos personales*; determinar quién es el responsable del tratamiento de datos; regular cuestiones esenciales del tratamiento de datos, tales como la conservación, el acceso, la seguridad, la confidencialidad; y determinar el nivel de protección adecuado para la transferencia de datos personales a otros países.

Son muchos los países del mundo que regulan la protección de datos personales para proteger los derechos de sus ciudadanos, y fomentar el desarrollo de empresas de servicios, cuyo objeto de negocios es la información. Así mismo, la protección

1. Las nociones sobre el derecho a la vida privada datan desde 1890 a partir de un artículo publicado por los juristas Samuel Dennis Warren y Louis Brandeis titulado "The right of privacy". En este artículo se establece la noción del derecho de todos los ciudadanos a hacer respetar su vida privada, en relación a nuevas tecnologías de la época como las fotografías en los periódicos, las imprentas. Disponible en ‹http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html›.
2. Francia, Declaración de Derechos Humanos, Asamblea General de las Naciones Unidas, 1948, art. 12.

de datos personales es fundamental para establecer políticas coherentes de gobierno electrónico, con un enfoque transnacional en donde el lenguaje jurídico debe estar a la par del desarrollo tecnológico.[3]

En el año 2015 propuse a la Asamblea Nacional la creación de una ley ecuatoriana de protección de datos personales. Aunque finalmente no fui tomado en cuenta para su elaboración, la Asamblea Nacional desarrolló un proyecto de ley titulado: "Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales". El proyecto fue archivado.

En este artículo haré una breve revisión del insuficiente marco jurídico actual sobre protección de datos personales en Ecuador, y, posteriormente, un análisis detallado de las principales falencias jurídicas que tuvo el proyecto fallido de la ley elaborada por la Asamblea Nacional.

MARCO JURÍDICO ACTUAL EN ECUADOR

La protección de datos personales en Ecuador está regulada de manera dispersa, imprecisa, y no está enfocada en los desafíos que presentan las tecnologías de la información. A continuación revisaremos las normas jurídicas sobre protección de datos personales que existen en Ecuador:

Constitución de la República del Ecuador

La Constitución instituye la protección de datos personales:

> 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.[4]

Se establece el derecho a la protección de datos personales, pero esta protección por sí sola es insuficiente por los siguientes motivos:

---

3. En la actualidad, varios gobiernos invierten en tecnologías distribuidas y redes P2P, con un nuevo enfoque del derecho a la vida privada. Ver, Government Office for Science, *Distributed Ledger Technology beyond Blockchain* (Londres: OGL, 2016), 47-53.
4. Ecuador, *Constitución de la República*, 2008, art. 66, num. 19.

- Es general: no provee una definición de datos personales, y deja muchos campos abiertos para la interpretación. Por ejemplo, al no especificar si la protección datos personales es solo para personas físicas, queda abierta la posibilidad de considerar a una persona jurídica como titular de derechos y garantías constitucionales.[5]
- No se establecen regulaciones, ni reglas preventivas: no existen reglas claras sobre el manejo de datos personales para las instituciones públicas y privadas, sean nacionales o extranjeras.
- No está enfocada en un medio transnacional como el internet: las empresas transnacionales que operan en el ciberespacio no están registradas en Ecuador. Esto dificulta enormemente la aplicación de medidas cautelares, sanciones, y el ejercicio de las garantías constitucionales tales como la acción de protección, y la acción de hábeas data.
- No establece una autoridad de protección de datos: es necesario crear un órgano público independiente que supervise el cumplimiento de las normas jurídicas sobre protección de datos personales.

Ley de comercio electrónico, firmas electrónicas y mensajes de datos

Esta ley provee la única definición sobre datos personales existente en la legislación ecuatoriana: "Datos personales: son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley".[6] Como podemos apreciar, es un concepto que no define de manera apropiada los datos personales.

Ley del sistema nacional del registro de datos públicos

Esta ley no define los *datos personales*, pero es muy importante considerarla como parte del engranaje donde tendrá que acoplarse la futura ley ecuatoriana referente a esta materia. Según esta ley, datos públicos son aquellos que constan en los registros de datos públicos, sin hacer una diferencia con datos personales protegidos:

---

5. La Sentencia No. 001-14-PJO-CC, 2011, marca un precedente en la jurisprudencia constitucional ecuatoriana, por medio del cual se planteó si es que las personas jurídicas también pueden considerarse como titular de los derechos protegidos por el recurso de hábeas data. Ver ‹http://www.uasb.edu.ec/web/observatorio-de-justicia-constitucional-del-ecuador/comentarios/-/journal_content/56/62017/991775›.
6. Ver, Congreso Nacional del Ecuador, *Disposiciones generales de la Ley No. 2002-67*, Ecuador, 2002.

> Art. 13.- De los registros de datos públicos.- Son registros de datos públicos: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual registros de datos crediticios y los que en la actualidad *o en el futuro determine la Dirección Nacional de Registro de Datos Públicos*, en el marco de lo dispuesto por la Constitución de la República y las leyes vigentes.[7]

Esta definición establece como facultad de la Dirección Nacional del Registro de Datos Públicos (DINADARP) el decidir los datos personales que serían considerados como datos públicos. Al no existir en el ordenamiento jurídico ecuatoriano una definición precisa de datos personales, esta facultad se vuelve discrecional. Esta ley entrará en conflicto directo con la futura ley de protección de datos personales, como será analizado posteriormente.

Código Orgánico Integral Penal

Como norma conexa, cabe mencionar que el Código Orgánico Integral Penal tipifica el delito de violación a la intimidad:

> La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, *difunda o publique datos personales*, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.[8]

Este artículo genera incertidumbre, por cuanto no existe aún en el ordenamiento jurídico ecuatoriano una definición precisa de *datos personales*.[9]

ANÁLISIS COMPARADO DEL PROYECTO DE LEY

Este acápite tiene como finalidad revisar las principales falencias que contiene el proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales: 1. las definiciones de datos personales, del responsable del tratamiento de datos personales, y del encargado del tratamiento; 2. La seguridad

---

7. Ecuador, *Ley del Sistema Nacional de Registro de Datos Públicos*, 2008, art. 13.
8. Ecuador, *Código Orgánico Integral Penal*, 2014, art. 18.
9. Si aplicásemos una interpretación gramatical estricta de este artículo, varias instituciones públicas ecuatorianas serían imputables por este delito.

y confidencialidad de los datos personales; 3. Autoridad de protección de datos personales; 4. Transferencia de datos personales a terceros países.

Para realizar el siguiente análisis, recurriremos a la situación actual en Ecuador, a la legislación comparada, y a la adaptación de las normas jurídicas a la luz de las tecnologías de la información.

Definición de datos personales

Los datos son una categoría muy amplia, por tanto se intentará extraer su esencia:

- Datos: información dispuesta de manera adecuada para su tratamiento por un ordenador.
- Metadatos: datos acerca de los datos. Ejemplos de metadatos son: la fecha de creación o modificación de un archivo, el encabezado de un email que contiene la ruta que siguió el mensaje, o la dirección IP[10] de origen.
- Protección de datos (enfoque técnico): consiste en salvaguardar la información, para evitar su pérdida o corrupción.
- Protección de datos personales (enfoque jurídico): la protección de datos personales es un mecanismo jurídico para proteger el derecho a la vida privada. En el mundo de hoy, toda actividad humana es traducida en datos digitales.

Revisemos algunas definiciones de datos personales:

a) Unión Europea

> Datos personales: toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.[11]

Revisemos algunos puntos importantes de esta definición:

---

10. Internet Protocol. Ver ‹http://www.alegsa.com.ar/Dic/direccion_ip.php›.
11. Reglamento (UE) 2016/679, *Unión Europea: Parlamento y Consejo Europeo*, 2016, art. 4.1. Cabe precisar que el Reglamento (UE) 2016/679, deroga a la Directiva 95/46/EC, y entrará en vigencia desde el año 2018.

- Sujeto de protección: solo aplica para personas físicas, y no para personas jurídicas. La protección de datos personales de personas jurídicas es tema actual de debate.
- Persona identificada: cuando se conoce de la persona su número de cédula de identidad, pasaporte, o cuando ya ha sido identificada mediante algún otro método.[12]
- Persona identificable: persona sobre la cual no se conoce su registro de identidad, pero puede llegar a ser identificable.
- Datos de localización: esto incluye de la manera directa a la geolocalización, a través de los Global Position Systems, u otros métodos de localización. De manera indirecta, también entrarían en esta categoría las direcciones IP,[13] y las cookies.[14]
- Identificador en línea: esta categoría sería aplicable a los servicios de identificación remota online, utilizados para verificar la identidad del usuario, a través de medios electrónicos de autenticación.[15]
- Identidad genética: considerar como datos personales a los genomas tiene un enorme impacto en el campo de la biotecnología y los datos referentes a la salud.

Como podemos apreciar, es una definición que está muy bien sincronizada con las tecnologías de la información.

b) Ecuador

Datos personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales identificadas o identificables: nombre y apellido, fecha de nacimiento, dirección domiciliaria, correo electrónico, número de teléfono, número de cédula, matrícu-

12. Por ejemplo, la identificación a través de métodos biométricos tales como el reconocimiento facial, o las huellas dactilares.
13. Internet Protocol. Ver ‹http://www.alegsa.com.ar/Dic/direccion_ip.php›.
14. Disponible en ‹http://www.alegsa.com.ar/Dic/cookie.php›.
15. Identificar no es lo mismo que autenticar. La autenticación por medios electrónicos tiene un enfoque técnico, y sirve para acreditar la supuesta identidad de una persona. Los métodos de autenticación se clasifican en tres categorías: 1. algo que se sabe; 2. algo que se es; 3. algo que se tiene. Ver en ‹https://www.owasp.org/index.php/Authentication_Cheat_Sheet_Espa%C3%B1ol›.

> la vehicular, información patrimonial e información académica o cualquier otra información vinculada con la identidad del titular.[16]

La primera parte de la definición es una copia casi textual de la definición europea. En la segunda parte, en lugar de utilizar categorías generales con respecto a la identidad, tales como identidad física o la identidad genética, los asambleístas ecuatorianos recurrieron a enumerar ejemplos de datos personales tales como el número de teléfono, o la matrícula vehicular, lo cual puede conllevar a errores de interpretación, y conflictos de leyes.

Consideremos las prácticas actuales de la administración pública. Todo individuo debe entregar una cantidad considerable de datos personales para obtener una factura con miras a deducir su impuesto a la renta. La factura incluye datos personales tales como su nombre, número de teléfono, dirección, entre otros. Esto genera que los datos de una persona estén guardados en instituciones públicas, farmacias, restaurantes, bares, gasolineras. Si bien, el contribuyente da su "consentimiento" a una institución como responsable del tratamiento de sus datos personales, la institución no debería compartirlos con otras instituciones, o publicarlos.[17]

La clave para esclarecer este conflicto será establecer un límite claro entre los datos públicos, y los datos personales como objeto de protección jurídica. Lo ideal hubiera sido elaborar una ley de protección de datos personales, y a partir de allí, determinar en qué circunstancias los datos personales se convierten en datos públicos. Lamentablemente en Ecuador sucedió al revés.

Responsable del tratamiento de datos

El tratamiento de datos son las operaciones que permiten procesar, conservar, transferir, registrar, o alterar los datos. Se considera como *tratamiento automatizado de datos* cuando los datos ingresan a los sistemas de información. Es decir, basta con que los datos personales sean escaneados, o enviados por email, chat, u otro medio electrónico, para que ya exista un tratamiento automatizado de datos.

Jurídicamente lo que nos interesa es determinar quién es el responsable del tratamiento de datos personales. Revisemos algunas definiciones:

---

16. Ecuador, *Proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales*, 2016, art. 4.3.
17. Como ejemplo, revisemos esta falta de cuidado en un portal web del CNT, en donde basta conocer un número de teléfono para acceder a datos personales de cualquier persona, los cuales deberían ser protegidos: Disponible en ‹http://soy.cnt.com.ec/cntapp/facturapdf/formulario.php›.

a) Unión Europea

"Responsable del tratamiento o responsable: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o junto con otros, *determine los fines y medios del tratamiento*...".[18]

b) Colombia

"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".[19]

La definición de la Unión Europea y la definición colombiana son coincidentes. El *responsable* es quien decide sobre el tratamiento de los datos. Para entender está definición es necesario aplicarla en determinados contextos:

- Ejemplo 1: si un individuo abre una cuenta en *Facebook* con sus datos personales, está confiando esta información a *Facebook*, por tanto este sería el responsable del tratamiento de datos.
- Ejemplo 2: si el individuo A publica en un sitio web datos personales del individuo B, el responsable del tratamiento de dicha información sería el individuo A.[20]

c) Ecuador

> Responsable del tratamiento de la información: persona natural o jurídica, pública o privada que sola o conjuntamente con otros, *administra el sistema de tratamiento de datos personales por cuenta del responsable del archivo, registro, base o banco de datos*. Toda operación de información que comprometa datos personales, en procedimiento mecánico o automatizado que tenga como fin la recolección, ordenamiento, conservación, almacenamiento, modificación, evaluación, destrucción, procesamiento de datos, así como el acceso de terceros por cualquier medio, deberá observar estrictamente la normativa prevista, bajo los derechos de protección y salvaguardia de identidad.[21]

---

18. Reglamento (UE) 2016/679, *Unión Europea: Parlamento y Consejo Europeo*, 2016, art. 4.7.
19. Colombia, *Ley Estatutaria No. 1581*, 2012, art. 3, inciso e.
20. Para reforzar este ejemplo, sugiero revisar el caso C-101/01, Lindquist, 6.11.2003. Disponible en ‹http://curia.europa.eu/juris/liste.jsf?language=es&num=c-101/01›.
21. Ecuador, *Proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales*, 2016, art. 4.7.

A la luz de las legislaciones de otros países, esta definición es inadecuada por los siguientes motivos:

- "*Administra el sistema de tratamiento de datos personales*": está disposición es imprecisa y resulta un misterio descifrar a que se refieren con "*sistema de tratamiento de datos personales*". En el supuesto de que se refieran a la administración de bases de datos, tengamos en cuenta que un administrador de bases de datos no es necesariamente el responsable del tratamiento de dichos datos, pues podría ser únicamente el encargado. Recordemos que en la actualidad, toda información ingresada y procesada por las aplicaciones web, se almacena en bases de datos de manera automática.
- "*Por cuenta del responsable del archivo, registro, base o banco de datos*": en esta disposición descubrimos que los legisladores intentaron más bien referirse al encargado del tratamiento de datos, y no al responsable del tratamiento de datos.

Encargado del tratamiento de datos

a) Unión Europea

"Encargado del Tratamiento o Encargado: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".[22]

b) Colombia

"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".[23]

En la Unión Europea y en Colombia, el encargado del tratamiento de datos actúa por cuenta del responsable. Para comprenderlo mejor, recurramos a los ejemplos previamente analizados:

---

22. Reglamento (UE) 2016/679, *Unión Europea: Parlamento y Consejo Europeo*, 2016, art. 4.8.
23. Colombia, *Ley Estatutaria No. 1581*, 2012, art. 3, inciso d.

- Ejemplo 1: si un individuo abre una cuenta con sus datos personales en *Facebook*, y *Facebook* los transfiere a *Twitter*, el encargado del tratamiento sería *Twitter*.
- Ejemplo 2: si el individuo A publica en *Facebook* datos personales del individuo B, el encargado del tratamiento sería *Facebook*.[24]

c) Ecuador

"Responsable del archivo, registro, base o banco de datos: persona natural o jurídica, pública o privada que es titular de un archivo, registro, base o banco de datos como custodio y operador de la información".[25]

No es una definición específica del *encargado del tratamiento* de datos. Sin embargo, podemos deducir que los legisladores confunden ciertos conceptos fundamentales. El *responsable de una base de datos* puede ser *responsable del tratamiento de datos*, y/o *encargado del tratamiento de datos*. Será el responsable si ha recibido la autorización de determinar los medios y fines del tratamiento por parte del titular de los datos personales. Será el encargado si realiza el tratamiento de datos por cuenta del responsable.

Seguridad y confidencialidad de los datos personales

a) Unión Europea

> Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
>
> a) la seudonimización y el cifrado de datos personales; b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; c) la capacidad de restaurar la disponibilidad y el acceso a los

---

24. Para profundizar la responsabilidad del encargado del tratamiento de datos, sugiero revisar el caso C-275/06, Promusicae, 29.1.2008. Disponible en ‹http://curia.europa.eu/juris/liste.jsf?language=es&num=C-275/06›.
25. Ecuador, *Proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales*, 2016, art. 4.8.

datos personales de forma rápida en caso de incidente físico o técnico; d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.[26]

- Seudonimización de datos personales: es una medida de protección que consiste en tratar los datos personales de manera que ya no puedan atribuirse a una persona en particular.[27] Esta medida ayuda a proteger otros derechos fundamentales de las personas físicas en varios campos, entre ellos podemos mencionar los exámenes académicos o las postulaciones laborales. Sin embargo, es un tema central de debate considerar a la *seudonimización* como medida suficiente de protección en ciertos campos, como el de la biotecnología.[28]
- El cifrado: es un método habitual en la criptografía, por el cual se codifica un mensaje a través de un algoritmo de cifrado,[29] para protegerlo. El cifrado es un método muy recomendable de protección de bases de datos que contengan datos personales, y para las transferencias de información.
- En cuanto a garantizar un nivel adecuado, el número 4 del mismo artículo establece: "La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un *mecanismo de certificación* aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo".[30]

Entre los estándares internacionales de seguridad más relevantes, tenemos:

- ISO 27001:2013: Buenas prácticas para el manejo de sistemas de información y proceso de datos.[31]
- PCI DSS: Transacciones y pagos con tarjetas de crédito.[32]
- OWASP ASVS: Seguridad de aplicaciones web.[33]

---

26. Reglamento (UE) 2016/679, *Unión Europea: Parlamento y Consejo Europeo*, 2016, art. 33.1.
27. Ibíd., art. 4.5.
28. Ver, Petra Bárd, Judith Sandor, "Anonymisation and Pseudonymisation as Means of Privacy Protection", en Katharina Beier, Silvia Schnorrer, Nils Hoppe, Christian Lenk, coord., *The Ethical and Legal Regulation of human tissue and biobank research in Europe* (Berlin: Universitätsverlag Göttingen, 2011), 35-45.
29. Disponible en ‹https://elbinario.net/2016/04/05/algoritmos-de-cifrado-i/›.
30. Reglamento (UE) 2016/679, *Unión Europea: Parlamento y Consejo Europeo*, 2016, art. 33.4.
31. Disponible en ‹http://www.iso.org/iso/catalogue_detail?csnumber=54534›.
32. Disponible en ‹https://www.pcisecuritystandards.org/pci_security/›.
33. Disponible en ‹https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project›.

b) Perú

La ley peruana de protección de datos distingue claramente lo que es la seguridad y lo que es la confidencialidad:

> *Seguridad del Tratamiento de Datos Personales*: para fines del tratamiento de datos personales, el titular del banco de datos personales de be adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado ... Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo.[34]
>
> *Confidencialidad de Datos Personales*: 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...[35]

La seguridad informática tiene un carácter técnico, y consiste en seguir buenas prácticas para mitigar riesgos y parchar vulnerabilidades en el manejo de la información, la infraestructura de redes, y el software. Cuando nos referimos a confidencialidad, más bien nos referimos a la confianza que tenemos en el responsable del tratamiento de datos, para que no haga pública la información protegida sin el consentimiento del titular de dicha información.

Esta diferencia entre seguridad y confidencialidad es fundamental al momento de determinar responsabilidades civiles y penales, tomando en cuenta el incremento de ataques informáticos, la vigilancia masiva de ciertos gobiernos a sus ciudadanos, y la falta de cuidado en el manejo de datos personales por parte de instituciones públicas y privadas.

c) Ecuador

El proyecto de ley ecuatoriano no regula la seguridad de manera específica. No regula la seudonimización, ni el cifrado, ni la aplicación de estándares de seguridad. Solo se menciona la seguridad y confidencialidad de manera superficial y general en algunos artículos.

Sin embargo, lo más preocupante en esta área, es lo establecido en el art 16:

---

34. Perú, *Ley de Protección de Datos Personales*, 2011, art. 16.
35. Ibíd., art. 17.

> *Inscripción registral*: todas las bases o bancos de datos, ficheros o archivos, en forma física o digital, de instancias públicas y las base o bancos de datos, ficheros, o archivos, en forma física o digital de empresas e instituciones privadas con fines exclusivamente financieros y mercantiles deberán inscribirse en el Registro Nacional de Bases de Datos Personales de acuerdo con los procedimientos y criterios que la Dirección Nacional de Registro de Datos Públicos establezca para el efecto.[36]

Según este artículo, el Estado tendría acceso y podría disponer de bases de datos que contengan datos personales de los ciudadanos en relación a sus transacciones mercantiles y financieras. Esta disposición es improcedente por las siguientes razones:

- El Estado ecuatoriano se convertiría en el primer infractor del derecho a la vida privada de los ciudadanos ecuatorianos, y de ciudadanos extranjeros cuya información sea transferida hacia servidores ecuatorianos.
- Está disposición legalizaría la vigilancia masiva del gobierno.
- Este mecanismo entorpecería la gestión de empresas, por cuanto las bases de datos hoy en día son dinámicas, y pueden cambiar en cuestión de segundos.
- Ni la Unión Europea ni ningún otro país que proteja los datos personales aceptarían esta norma jurídica. Con ello, el Ecuador ratificaría su condición de país que no ofrece un nivel adecuado de protección para recibir transferencias de datos personales desde el extranjero.

Autoridad responsable de la protección de datos personales

Es potestad de los Estados el delegar una autoridad la competencia para hacer efectiva la tutela de los derechos establecidos en las leyes de protección de datos personales. En la Unión Europea, el Reglamento 2016/679 delega dicha responsabilidad a cada miembro de la Unión, pero recomendando la independencia de dicha autoridad.

a) España

La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá

36. Ecuador, *Proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales*, 2016, art. 16.

por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.[37]

La autoridad de protección de datos personales está concebida como un ente de derecho público. En España es independiente. En Colombia depende de la Superintendencia de Industria y Comercio, a través de una delegatura para la protección de datos personales.[38] En Perú depende del Ministerio de Justicia, a través de la Dirección Nacional de Justicia.[39]

b) Ecuador

En nuestro país, el artículo 11 del proyecto de ley asigna la autoridad de protección de datos a la Dirección Nacional de Registro de Datos Públicos, órgano adscrito al Ministerio de Telecomunicaciones y Sociedad de la Información.

> Art. 11.- "Autoridad Nacional de Protección de Datos Personales. La Dirección Nacional de Registro de Datos Públicos adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información será la Autoridad Nacional de Protección de Datos Personales y ejercerá la vigilancia y control para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley.[40]

Tal como está planteado el proyecto, la Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales entraría en conflicto directo con la Ley del Sistema Nacional del Registro de Datos Públicos. En caso de conflicto de leyes, al menos en teoría, prevalecería la ley orgánica, aunque podríamos predecir que será necesaria una reforma.

Sin embargo, es preciso cuestionarse acerca de si la DINADARP es realmente el órgano adecuado para proteger y ejercer la tutela de los datos personales. En teoría, la nueva ley orgánica pondría un impedimento a la facultad de la DINADARP para decidir qué datos son considerados como datos públicos. Pero, al ser el mismo organismo público el que decide la diferencia entre datos personales y datos públicos, su imparcialidad podría ser cuestionable.

---

37. España, *Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*, 1999, art. 35.
38. Colombia, *Ley Estatutaria No. 1581*, 2012, art. 19.
39. Perú, *Ley de Protección de Datos Personales*, 2011, art. 32.
40. Ecuador, *Proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales*, 2016, art. 11.

Transferencia de datos personales a terceros países

Las transferencias internacionales de datos personales suceden cuando los datos de ciudadanos o residentes un país, son transferidos, para ser tratados en otro país. Para ello debe haber un exportador de datos y un importador de datos.

En la era de la información que vivimos, las transferencias de datos suceden todo el tiempo: cuando utilizamos redes sociales, cuando utilizamos servicios en la nube, cuando comentamos en foros, cuando utilizamos el chat, cuando utilizamos motores de búsqueda, cuando hacemos transacciones en la blockchain,[41]programas P2P,[42] etc.

a) Unión Europea

> Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.[43]

b) Argentina

"Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados".[44]

La regulación europea y la ley argentina coinciden en exigir un nivel adecuado de protección para la transferencia de datos a otros países. En este punto, la clave es entender lo que implica tener un nivel adecuado de protección. En la Unión Europea, la Comisión Europea decide qué países ofrecen un nivel adecuado de protección de acuerdo a su legislación interna, y a los acuerdos internacionales que haya suscrito en materia de protección de datos personales. El proceso de aprobación incluye una

41. Disponible en ‹http://www.blockchaintechnologies.com/blockchain-glossary›.
42. Peer to Peer. Disponible en ‹https://techterms.com/definition/p2p›.
43. Reglamento (UE) 2016/679, *Unión Europea: Parlamento y Consejo Europeo*, 2016, art. 45.1.
44. Argentina, *Ley No. 25326*, 2000, art. 12.

proposición de la Comisión, opiniones de los estados miembros, y una aprobación por parte de un comité especializado en la materia.[45]

Entre los países latinoamericanos que constan en esta lista están Argentina, desde el año 2003, y Uruguay, desde el año 2012. La ventaja de constar en esta lista es poder realizar transferencias de datos directas, sin requerir la autorización por parte de la autoridad de protección de datos personales por parte del país exportador de datos. Esto ayuda enormemente al desarrollo de las empresas que operan en internet cuyo objeto de negocios es la información, y están sujetos a cumplir con lo establecido por las legislaciones de múltiples países.

Como dato adicional, cabe mencionar que Estados Unidos no ha sido considerado como un país con un nivel adecuado de protección. Por ello se creó el acuerdo de Safe Harbor,[46] estableciendo principios de privacidad que debían cumplir las empresas estadounidenses para procesar datos personales provenientes de los países de la Unión Europea. La Corte de Justicia Europea declaró este acuerdo como inválido en octubre de 2015, a raíz del caso de Max Schrems contra Facebook.[47]

Es así que un nuevo acuerdo denominado Privacy Shield[48] fue aprobado el 8 de julio de 2016, ampliando los principios que deben cumplir las empresas estadounidenses para certificarse y poder realizar el tratamiento automatizado de datos provenientes de la Unión Europea.

c) Ecuador

"Prohibición: Se prohíbe la transferencia de datos personales de cualquier tipo a países u organismos internacionales que no proporcionen niveles de protección de datos, conforme con las normas de derecho internacional o regional en la materia".[49]

El Ecuador no es considerado como país que ofrece un nivel adecuado de protección a los datos personales, ni por la Unión Europea, ni por ningún otro país del mun-

---

45. Disponible en ‹https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php›.
46. Disponible en ‹http://2016.export.gov/safeharbor/›.
47. Probablemente este es el precedente jurídico internacional más importante en lo que concierne a la transferencia internacional de datos personales. Disponible en ‹http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf›.
48. Disponible en ‹http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf›.
49. Ecuador, *Proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales*, 2016, art. 20.

do. El proyecto de ley de protección de datos ecuatoriano no cumple con los requisitos establecidos por la Unión Europea, sobre todo considerando el artículo 16 por el cual el Gobierno ecuatoriano crearía un registro de bases de datos.

CONCLUSIONES

El Ecuador necesita de urgencia una ley de protección de datos personales para proteger el derecho a la vida privada de sus ciudadanos, y promover el desarrollo de empresas ecuatorianas de servicios en internet, que puedan tratar datos de ciudadanos de todo el mundo.

El proyecto de ley elaborado por la Asamblea Nacional fue una iniciativa importante, pero lamentablemente contuvo falencias jurídicas que deberán ser corregidas en una futura ley ecuatoriana de protección de datos personales.

Para superar sus falencias jurídicas, es necesario que los asambleístas lleguen a comprender la naturaleza transnacional de esta área jurídica, y la necesidad de contar con la asesoría adecuada en temas de tecnologías de la información.

Finalmente, quisiera destacar también que este proyecto de ley fue mediatizado en vísperas del proceso electoral del año 2017. Considero que fue el tiempo equivocado, por cuanto la opinión pública abordó el tema de la protección de datos personales de manera política, y no jurídica.

¡Borrón y cuenta nueva!

BIBLIOGRAFÍA

Bárd Petra, Judith Sandor. "Anonymisation and Pseudonymisation as Mens of Privacy Protection". En Katharina Beier, Silvia Schnorrer, Nils Hoppe y Christian Lenk, coord., *The Ethical and Legal Regulation of Human Tissue and Biobank Research in Europe*. Berlin: Universitätsverlag Göttingen. 2011.

Government Office for Science. *Distributed Ledger Technology: beyond Blockchain*. Londres: OGL, 2016.

Laudati, Laraine. *ECJ Decisions Relating Data Protection*. Unión Europea: OLAF DPO, 2015.

Lorica, Ben. "Data Analysis: Just One Component of The Data Science Workflow". En *Big Data Now 2013*. Estados Unidos: O'Reilly Inc., 2013.

Warren, Samuel, y Louis Brandeis. "The right of privacy". *Harvard Law Review* 4, No. 5 (1890).

Normativa

Argentina. *Ley No. 25326*. 2000.

Colombia. *Ley Estatutaria No. 1581*. 2012.

Directiva 95/46/CE. 1995. Unión Europea: Parlamento y Consejo de la Unión Europea.

Ecuador. *Código Orgánico Integral Penal*. *Registro Oficial*, No. 180, 10 de febrero de 2014.

Ecuador. *Constitución de la República*. *Registro Oficial*, No. 449, 20 de octubre de 2008.

Ecuador. *Ley del Sistema Nacional de Registro de Datos Públicos*. 2008.

Ecuador. *Proyecto de Ley Orgánica de Protección de los Derechos a la Intimidad, y Privacidad sobre los Datos Personales*. 2016.

EU-US privacy shield framework principles. 2016. Estados Unidos: US department of commerce.

España. *Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*. 1999.

Ley de Protección de Datos Personales. 2011. Perú: Congreso de la República del Perú.

Reglamento (UE) 2016/679. 2016. Unión Europea: Parlamento y Consejo de la Unión Europea.

Jurisprudencia

Ecuador, Corte Constitucional. Sentencia No. 001-14-PJO-CC, 2011.

Unión Europea, Tribunal de Justicia. Caso C-101/01, *Lindquist*, 2003.

Unión Europea, Tribunal de Justicia. Caso C-275/06, *Promusicae*, 2008.

Unión Europea, Tribunal de Justicia. Caso C-362/14, *Maximiliam Schrems v. Data Protection Commissioner*, 2015.

Fecha de recepción: 10 de febrero de 2017
Fecha de aprobación: 27 de abril de 2017

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador

*Lorena Naranjo Godoy**

RESUMEN

El número 19 del artículo 66 de la Constitución de la República del Ecuador (CRE) señala como presupuesto del derecho a la protección de datos personales tanto al dato como a la información de un individuo. Sin embargo, la jurisprudencia ecuatoriana requiere para su procedencia que estos tengan un carácter informativo. Asimismo, el artículo 92 de la CRE referente al hábeas data señala como supuestos de protección a los documentos, datos genéticos, bancos o archivos de datos personales e informes sobre sí misma, o sobre sus bienes. Estos criterios lejos ser abarcadores, pueden no respetar los componentes del derecho a la protección de datos personales y, por el contrario, causar confusión e incluso no ser pertinentes para garantizar la tutela del derecho a la protección de datos personales.

Palabras clave: protección de datos personales, hábeas data, dato personal, información personal.

ABSTRACT

The Ecuadorian Constitution on its Article 66 - numeral 19 recognizes the datum itself and the personal information as objects of the right to protection of personal data. However, to acknowledge that protection, the Ecuadorian jurisprudence requires the data to have an informative purpose. Likewise, while Article 92 of the Ecuadorian Constitution recognizes documents, genetic data, banking information, personal data files and information about goods as elements to be protected by habeas data; that list of elements may not be enough to explain the spirit of the right to protection of personal data and may cause confusion or even not be effective to guarantee the right.

Keywords: protection of personal data, hábeas data, personal datum, personal information.

* Directora de la Escuela de Derecho de la Universidad de las Américas, Ecuador (UDLA).

INTRODUCCIÓN

El vertiginoso avance de las tecnologías de la información y la comunicación provocan en las sociedades nuevas formas de transgresión de derechos fundamentales. Por lo tanto, es indispensable avanzar con precisión y celeridad en la configuración de nuevos derechos y en el reconocimiento de distintos e innovadores contenidos o enfoques de aquellos existentes. Pero además es necesario que las garantías constitucionales y legales que los tutelan vayan acoplándose a estas nuevas prerrogativas o a sus nuevos dimensionamientos, de tal manera que, paulatinamente, pueda perfeccionarse un adecuado sistema de amparo.

El objetivo de este artículo es estudiar el alcance y las dimensiones o limitaciones de los *datos o información de carácter personal* como presupuestos de uno de los derechos más importantes de la era digital, el denominado protección de datos personales.

En el caso de Ecuador, su reconocimiento se produce a través del número 19 del artículo 66 de la Constitución de la República, aunque las primeras formas aproximadas de resguardo se originaron con la inclusión del hábeas data en las reformas de 1996 a la Constitución de 1978.

Mediante el análisis exegético la normativa constitucional –ya que no existe una ley específica que aclare esta cuestión– y de la revisión de la interpretación jurisprudencial, se examinará si la forma en la que se han contemplado estos presupuestos faculta la efectiva vigencia de este derecho fundamental. Además, verificar la procedencia de la garantía constitucional del hábeas data como mecanismos constitucional que viabilice su ejercicio.

Asimismo, se identificará si los criterios de garantía descritos en la acción de hábeas data y que constan en el artículo 92 de la CRE son pertinentes para proteger este derecho o deben adaptarse a su naturaleza. Para aclarar esta temática se vuelve indispensable analizar los conceptos de: datos e información de carácter personal, para luego contrastarlos, asimilarlos, integrarlos o excluirlos de aquellos descritos en el mencionado artículo 92 de la CRE como: documentos, datos genéticos, bancos o archivos de datos personales e informes sobre sí misma, o sobre sus bienes.

Para cumplir con las finalidades planteadas se propone una estructura en la que se aborde la naturaleza jurídica del dato personal como presupuesto del derecho a la protección de datos personales en la doctrina y el derecho comparado, para lo cual se revisarán los orígenes y antecedentes del derecho. Posteriormente se revisará el reconocimiento del derecho y sus componentes en la normativa y jurisprudencia constitucional ecuatoriana. Finalmente, se analizarán los términos: documentos, datos genéticos, bancos o archivos de datos personales e informes, en la garantía constitucional

de hábeas data; para concluir que existen divergencias entre la doctrina, la legislación comparada, la legislación nacional y la posición adoptada por la jurisprudencia constitucional del Ecuador, que, aunque no es vinculante, podría limitar el ejercicio del derecho en cuestión.

ANTECEDENTES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

La necesidad de proteger todos los datos relativos a las personas no es algo anecdótico, pues ellos representan el registro de su vida, reflejan sus características, sus opciones vitales, sus debilidades. El tratamiento adecuado de los datos personales es una exigencia de la dignidad de la persona y del libre desarrollo de la personalidad, algo especialmente necesario en la etapa de desarrollo de la personalidad, de formación del carácter y de los valores personales. El conocimiento por parte de otros de una información que una persona no ha querido revelar afecta seriamente a la forma en que esta se desenvuelve normalmente en la sociedad, la manera en que es vista por sus familias, por sus vecinos, o por sus compañeros de trabajo.[1]

Los avances tecnológicos han permitido su difusión masiva, situación que pone en riesgo a las personas y aumenta exponencialmente los daños a sus derechos fundamentales.

Tiene su evidente nacimiento en un mundo tecnificado y globalizado, en el que la ingente generación de sistemas, procesos de decisión, así como a través de tratamientos sencillos, de procesos automatizados o incluso de minería de datos,[2] pueden otorgar perfiles de personalidad que pueden usarse para provocar transgresiones no solo a la privacidad sino a otros derechos fundamentales.

El derecho a la protección de datos personales tiene su origen en la intimidad, del que se separa gradualmente hasta que se reconoce su autonomía a través de la jurisprudencia y posteriormente de la incorporación de normativa constitucional, legal e incluso reglamentaria. Inicialmente, por su antecedente inmediato se atendía únicamente datos considerados íntimos, o aquellos que tenían un nivel adicional de protec-

1. Antonio Troncoso Reigada, *La protección de datos personales: en busca del equilibrio* (Valencia: Tirant lo Blanch, 2010), 32.
2. El profesor Aluja utiliza la definición de minería de datos ya adelantada por Hans (1998): "el proceso de análisis secundario de grandes bases de datos con el objetivo de encontrar relaciones insospechadas que son de interés o aportan valor al titular de la base de datos". Tomás Aluja, "La minería de datos, entre la estadística y la inteligencia artificial", *Qüestiió* 25, No. 3 (2001).

ción, los denominados datos sensibles, que "permitan identificar a la persona, confeccionando su perfil ideológico, racial, sexual, económico, o de cualquier otra índole".[3]

Posteriormente, también se resguardaron aquellos datos personales considerados irrelevantes, ya sean estos pasados, presentes e incluso futuros, ya que a través de su recopilación, almacenaje y tratamiento paulatino, pueden asociarse para entregar perfiles completos de las personas.

> Por lo tanto, no importa si los datos parecieran a priori irrelevantes, pueden servir para una finalidad diferente y, por lo tanto, proporcionan claves insospechadas sobre la persona... La teoría del mosaico pone de relieve como datos aparentemente inocuos pueden aportar una información preciosa a la hora de elaborar un determinado perfil personal. Por tanto, todos aquellos datos referentes a la persona merecen la protección que otorga la Ley.[4]

En cualquier caso, no se protegen los datos en sí mismos, sino a los titulares de esos datos. El objeto de resguardo es la autodeterminación informativa, que consiste en la libertad de un titular respecto de cómo disponer de sus datos personales, cualquiera sea la naturaleza de estos, es decir, no solo aquellos referidos al ámbito de su intimidad o privacidad, sino incluso los aparentemente inocuos, con miras a desarrollar un proceso de autoconstrucción de su personalidad en sociedad, y replicar las consecuencias indeseadas de valoraciones no deseadas, no autorizadas, equivocadas o inexactas.

En consecuencia, debe atribuirse mayores niveles y garantías de protección a los datos personales, "es conveniente insistir en que la protección de datos personales es también un instituto de garantía de otros derechos fundamentales",[5] ya que la influencia y repercusión de la recopilación, tratamiento y difusión de los datos personales afectan directamente el ejercicio de las libertades individuales en una sociedad en la que lo virtual y lo real se interrelacionan constantemente.

---

3. Concepción Conde Ortiz, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad* (Madrid: Dykinson, 2005), 66.
4. María Luisa Fernández Esteban, "Nuevas tecnologías, internet y derechos fundamentales" (Madrid: MacGraw-Hill, 1998), 129.
5. Ibíd., 37.

NATURALEZA JURÍDICA DEL DATO PERSONAL COMO PRESUPUESTO GENERALIZADO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Una vez determinado que el derecho a la protección de datos personales protege no solo al dato íntimo, sino también el inocuo, es necesario establecer la naturaleza jurídica del dato y de la información personal, para lo cual se recurrirá como referente inmediato a la Unión Europea, con énfasis en España, por ser su Corte Constitucional y su Agencia de Protección de Datos Personales[6] líder en los principales avances en el contenido esencial y eficacia real de este derecho.

Concepto de datos de carácter personal

La Directiva 95/46/CE en su artículo 2 relativo a las Definiciones señala que: "A efectos de la presente Directiva, se entenderá por: a) 'datos personales': toda información sobre una persona física identificada o identificable".[7] El artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal española, que es manifestación de la Directiva Europea señala idéntica definición de datos de carácter personal.

Asimismo, la letra f) del artículo 5 del Reglamento de desarrollo de la Ley Orgánica 15/1999, al determinar las definiciones aplicables dice que: "Definiciones. 1. A los efectos previstos en este reglamento, se entenderá por: f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".[8]

Las normas que regulan el derecho en cuestión conceptualizan al dato como información. Si bien originalmente se consideraba que solo ameritaba protección la información y no el dato, ya que "la información hace referencia, pues, a datos estructurados y seleccionados para un usuario, una situación, un momento y un lugar. Mientras no sean evaluados o aplicados a un problema específico, los datos seguirán siendo

---

6. Troncoso Reigada, *La protección de datos personales*, 2.
7. Europa: 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.
8. España: Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

solo datos, es decir, símbolos con poco o ninguna significado".[9] Es decir, se consideraba que el dato "no explica el porqué de las cosas y en sí mismo no significa nada [mientras que] la información es el significado que una persona le asigna a un dato".[10]

Sin embargo, esta visión se encuentra superada pues se protege al dato porque de él se extrae información. En consecuencia, este derecho resguarda toda posible vulneración que puede producirse no solo respecto de la información de un individuo sino de sus datos o incluso de fragmentos de estos, pues a través de procesos de tratamiento pueden delinearse perfiles de un individuo. Es decir, se protege al dato por la sola posibilidad de que pueda llegar a tener una significación, es decir convertirse en información.

Las normas citadas utilizan la frase *cualquier*, o la generalización *todo*, señalando que no queda por fuera del ámbito de protección ningún tipo de dato ni de soporte sea este físico o virtual.

Por lo tanto, podemos señalar que se considera dato personal a toda información numérica, alfabética, también imágenes (gráfica y fotográfica), acústica (sonidos y voces) o cualquier otro de tipo de información con las condiciones de que puedan ser recogidas, registradas, tratadas o transmitidas y que pertenezcan a una persona física identificada o identificable. Se anota que no solo se refiere a datos habituales o comunes, sino incluso a aquellos que la persona desconozca sobre sí misma,[11] en virtud de la existencia de tratamientos como la minería de datos.

Es indispensable la comprensión ampliada de este concepto, pues permite aclarar dudas respecto de cierto tipo de datos que por sus características no se tiene la certeza de su condición de personales y, en consecuencia, debe analizarse si están sujetos o no a esta normativa, toda vez que existen dudas respecto de su vinculación a un individuo. Por ejemplo: la dirección de correo electrónico, web e IP, los log-in de acceso, los SMS, los datos de fallecidos, del *nasciturus*. Asimismo, existe un grupo de datos de los que no existe vacilaciones respecto de su naturaleza, sino que sus elementos definitorios determinan la necesidad de un régimen de protección blindado, como por ejemplo: datos sensibles, datos genéticos, datos de salud, datos obtenidos en sistemas de videovigilancia, entre otros.

---

9. R. H. Saroka, *Sistemas de información en la era digital* (Buenos Aires: Fundación Osde, s. f.), citado por Aníbal Pardini, "La información y su sistema de protección", *Revista de Direito Do Comércio Internacional Temas E Atualidades Internet, Comércio Eletrônico E Sociedade Da Informação* (2006): 22.
10. Ibíd., 22.
11. Isabel Davara Fernández de Marcos, *Hacia la estandarización de la protección de datos personales: propuesta sobre una "Tercera Vía O Tertium Genus" Internacional* (Madrid: La Ley, 2011), 141.

Identificativo o identificable

Conforme señala el artículo 2, letra a) de la Directiva 95/46/CE se consideran datos personales:

> toda información sobre una persona física identificada o identificable ("el interesado"); 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 y social.

En el mismo sentido, el Real Decreto 994/1999 español de 11 de junio que aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que a efectos de definir que debe entenderse por identificación, señala: "5. Identificación: procedimiento de reconocimiento de la identidad de un usuario".

En conclusión, son datos identificativos aquellos que permiten una atribución directa como nombres, dirección, teléfono, número de cédula, pero también aquellos que se pueden sumar a los identificativos para someterlos a tratamiento [...] datos de características personales, datos de circunstancias sociales, datos académicos y profesionales, datos de detalles de empleo, datos de información comercial, datos económicos-financieros, datos de transacciones y datos especialmente protegidos".[12]

En cambio, son datos identificables:

> Aquellos que para los que no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados y 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.[13]

Otras recomendaciones del Consejo de Europa señalan además que una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas. Si una persona natural no fuere identificable, los datos se considerarán anónimos.[14] Si bien estos conceptos resultan ambiguos, se puede concluir

---

12. Daniel Santos García, *Nociones generales de la Ley Orgánica de Protección de Datos y su Reglamento: adaptado Al RD 1720/2007 de 21 de diciembre*, 2a. ed. (Madrid: Tecnos, 2012), 42.
13. SAN recurso 948/2000, de 8 de marzo de 2002.
14. Consejo de Europa, "Recomendación No. R (97) 18 y exposición de motivos del Comité de Mi-

naturalmente que "no es lo mismo que se identifique a una persona utilizando criterios de búsqueda en el marco de un sistema automatizado, que a través de los documentos, que se disponga en soporte papel".[15]

Asimismo, si los datos se someten a un proceso de disociación, por el cual no es posible la identificación de su titular o afectado, se pierde la característica fundamental de su vinculación personal y se vuelven anónimos. Por lo tanto, los datos personales anonimizados dejan de estar bajo la égida del derecho a la protección de datos personales porque "cualquier información, en cuanto asociada a un titular, es información de carácter personal, no por la información en sí, sino por su asociación con la persona física a la que se protege".[16]

En consecuencia, los datos o información se protegen por su vinculación con una persona. Esta vinculación puede ser directa (datos identificativos) o indirecta (datos identificables). Su amparo es indispensable porque se protege la autodeterminación informativa de la persona.

RECONOCIMIENTO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LA NORMATIVA ECUATORIANA

La Constitución de 2008 es la primera que reconoce el derecho a la protección de datos personales en Ecuador, y lo hace desde el enfoque europeo, con la voluntad de cumplir un alto estándar de protección. El mencionado número 19, artículo 66 de CRE, describe perfectamente uno de los contenidos esenciales del derecho, el relativo a la autodeterminación informativa.[17] No solo prescribe el *acceso* a los datos, como constaba en su antecedente inmediato, el hábeas data, tanto en la Constitución de 1978, codificada en 1996, como en la Constitución de 1998, sino la *decisión* sobre su información.

En consecuencia, el objetivo fundamental del derecho a la protección de datos personales en Ecuador es proteger la autodeterminación informativa de la persona.

---

nistros a los Estados Miembros relativa a la protección de datos de carácter personal, recogidos y tratados con fines estadísticos", 30 de septiembre de 1997, 3.

15. Juan Zabía de la Mata e Irene Ma. Agúndez Lería, edit., *Protección de datos: comentarios al reglamento* (Valladolid: Lex Nova, 2008), 112.
16. Davara Fernández de Marcos, *Hacia la estandarización de la protección de datos personales*, 147.
17. "Según la elaboración alemana, la autodeterminación informativa, en el marco de la personalidad, podría definirse como el derecho del individuo a controlar la obtención, tenencia, tratamiento y transmisión de datos relativos a su persona". María Mercedes Serrano Pérez, *El derecho fundamental a la protección de datos. Derecho español y comparado* (Madrid: Thomson / Civitas, 2003), 67.

No existe confusión con el derecho a la intimidad o con la privacidad. Se protege todo tipo de datos personales y se supera la determinación histórica, dependiente y atada al derecho a la intimidad que protegía únicamente el dato íntimo, privado, reservado, personal, familiar o sensible, como consta equivocadamente en la normativa legal,[18] pues los datos inocuos o irrelevantes también gozan del estatus de protección, toda vez que cualquiera de estos, dependiendo de los tratamientos, procesamientos o formas de difusión, pueden potencialmente afectar el libre desarrollo de la personalidad de un individuo y el ejercicio de otros derechos fundamentales.

La doctrina, normativa y jurisprudencia internacional generalmente tiene una configuración aceptada como concepto. Sin embargo, cada país puede establecer sus propias formas de comprensión acerca de la institución o de la naturaleza jurídica de un presupuesto de derecho, como es el caso de los datos e información de carácter personal. Es menester analizar los elementos comunes entre la visión ampliamente aceptada y las especificidades de nuestra normativa y verificar si estas son efectivas, de tal forma que no necesiten interpretaciones o reformas, o, por el contrario, sea necesario intervenir ya sea a través de propuestas normativas o reglamentarias que aclaren dudas, eviten confusiones y en suma permitan materializar este derecho fundamental.

Este artículo se enfocará en definir la naturaleza jurídica del dato o información de carácter personal en Ecuador desde la normativa constitucional, y de la jurisprudencia existente (*obiter dicta*), pues solo a través de una adecuada delimitación se puede determinar los ámbitos de protección y exclusión de este derecho fundamental, toda vez que no todos los datos ameritan un sistema de protección especializado, sino únicamente los de carácter personal, pues permite salvaguardar al individuo desde distintas perspectivas: derechos intimidad, privacidad, libre desarrollo de la personalidad, autodeterminación informativa e incluso en el ejercicio de otros derechos fundamentales; además, verificar la procedencia de la garantía constitucional del hábeas data que viabilice su ejercicio.

---

18. *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos* publicada en el *Registro Oficial* 557-S, 17 de abril de 2002, art. 9: "...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".

NATURALEZA JURÍDICA DEL DATO PERSONAL EN LA NORMATIVA ECUATORIANA

En el análisis de los elementos que conforman el concepto de dato personal en la normativa ecuatoriana es menester investigar si en la normativa o en la jurisprudencia se recogen aquellos criterios que han sido desarrollados por la normativa y jurisprudencia internacional.

Al respecto, corresponde analizar el derecho fundamental a la protección de datos personales que consta en el artículo 66, número 19 de la CRE, que formula:

> 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

De tal forma que se deben estudiar los siguientes elementos:

Datos e información

De la simple lectura del artículo se colige que se usan los términos *datos e información* como si se tratasen de sinónimos, aunque no lo son. Tanto en la normativa, como en la jurisprudencia internacional no suele utilizarse el término información sino únicamente el vocablo *dato* por considerar que de este puede extraerse información y que es lo suficientemente amplio para incluir en él cualquier: a) soporte: físico o virtual; b) tipo de manifestación: gráfica, acústica o fotográfica; c) pauta de expresión: numérica o alfabética; y, en general, d) por la diversidad y asociación de la fuente al individuo: como ha ocurrido en otros países donde, paulatinamente, se ha reconocido la condición de dato personal a las direcciones IP, los *clicks* de un usuario, el *log in* a un sitio web, datos biométricos, entre otras.

Sin embargo, respecto de las diferencias entre dato e información la sentencia No. 001-14-PO-CC de 3 de julio de 2014, dictada por la Corte Constitucional ecuatoriana en su parte argumentativa –que no genera una regla de aplicación obligatoria sino que marca un criterio referencial para orientar la interpretación judicial–, señala:

> Sin embargo, se ha identificado en la doctrina sobre la protección de datos una distinción entre los conceptos "dato" e "información" a la que se adscribe esta Corte, como lo relata Osvaldo Gozaíni: Algunos entienden "datos" a la representación de hechos, conceptos o instrucciones bajo una forma adaptada a la comunicación, a la interpretación o al tratamiento por seres humanos o máquinas, y por "informaciones" al significado que toman

> los datos de acuerdo con convenciones vinculadas a estos. De acuerdo con la distinción conceptual citada, el dato adquiere la calidad de información en tanto cumple una función en el proceso comunicativo.[19]

En la jurisprudencia ecuatoriana, la diferenciación entre dato e información no alude al soporte, al tipo de manifestación, a la pauta de expresión o a la diversidad de la fuente, sino a su funcionalidad como medio para establecer una evaluación, apreciación o simbolización del dato, que lo caracteriza como información. La mencionada sentencia alude a esta diferenciación:

> La información, entonces, requiere una interpretación del dato, que dota de carga valorativa y funcionalidad concreta a la descripción que este hace. Por lo tanto, el dato solamente es relevante para la protección por medio del hábeas data, en la medida en que sea susceptible de cumplir una función informativa. El mismo autor explica dicho proceso de la siguiente manera: El dato es difícil que, por sí solo, pueda tener una incidencia grande o grave en la llamada privacidad. Esto es, mientras el dato no resuelva una consulta determinada, no sirva a un fin, no dé respuestas o no oriente la posible solución a un problema, es el antecedente o punto de partida para la investigación de la verdad; pero, en el momento en que ese mismo dato da respuesta a una consulta determinada, o sirve a un fin, o se utiliza para orientar la solución de un problema, se ha convertido en información. Como conclusión, los datos están protegidos por medio de la garantía constitucional del hábeas data, siempre que cumplan con una función informativa respecto de las personas y sus bienes y por ende, su comunicación, interpretación o tratamiento afecta en mayor o menor medida los derechos de aquel a quien se refieren.[20]

La sentencia transcrita concluye que, para los jueces constitucionales ecuatorianos, el dato en sí mismo no es objeto de la acción de hábeas data sino únicamente aquel que puede llegar a cumplir una finalidad informativa, y que en efecto se convierte en información. Esta aseveración debe ser adecuadamente contextualizada, ya que no puede significar que el derecho a la protección de datos se vea limitado o restringido a proteger únicamente información personal. Esto debido a que, para que el régimen de protección sea completo, el número 19 del artículo 66 de la CRE invoca expresamente los dos términos: tanto *dato* como *información*. Toda vez que el derecho a la protección de datos personales salvaguarda también los datos personales por sí mismos, en la medida en que –aunque aparentemente irrelevantes y carentes de contenido informativo– pueden o tienen el potencial de ser sometidos a un proceso o tratamiento

---

19. Ecuador. Corte Constitucional (Sentencia No. 001-2014-PJO-CC), *Gaceta Constitucional* No. 007, 3 de julio de 2014.
20. Ibíd.

que proporcione un perfil completo de un individuo. Precisamente, por este motivo es indispensable implementar mecanismos preventivos como registro de la existencia de bases de datos, sus finalidades y cesiones; así como controles de verificación a los responsables de ficheros respecto del cumplimiento de los principios como calidad, consentimiento informado, seguridad de la información, entre otros, por parte de entidades especializadas. Es decir, el derecho a la protección de datos personales también tiene como objetivo prevenir posibles tratamientos que pudieran generar un daño.

La posición jurisprudencial de que el hábeas data limite su protección a los datos informativos o con función informativa, puede provenir de que esta garantía jurisdiccional protege otros derechos, como el honor, el buen nombre, la intimidad personal y familiar.[21] En este sentido, para la transgresión de estos evidentemente se necesita de un dato que genere una evaluación o valoración en un contexto social, familiar o íntimo que cause un daño a la persona. Sin embargo, el hábeas data también es garantía del derecho a la protección de datos personales, por lo que debe adaptarse al contenido esencial del derecho que tutela, y, en este sentido, también se incluye en su ámbito de protección al dato por sí solo, aunque inicialmente carezca de la característica informativa, porque incluso aquel dato que en apariencia no afecta a la privacidad, al decir de la citada sentencia, una vez tratado por medios automatizados puede en conjunto otorgar una visión integral de un individuo que no solo afecten su intimidad, sino incidir directamente en el ejercicio de otros derechos fundamentales. En suma, la conclusión que consta en esta sentencia, y que para la jurisprudencia se reconoce como *obiter dicta*, debe utilizarse como mecanismo orientador únicamente en aquellos contextos que le son aplicables.

Datos de carácter personal

La norma deja expresa constancia de la condición de que el dato debe estar vinculado a un titular para ser considerado de carácter personal. La norma constitucional no hace alusión a si esta forma de asociación entre el dato y el individuo es directa o indirecta, por lo que los elementos de identificado e identificable no han sido desarrollados en la versión ecuatoriana, aunque es común en la mayoría de los ordenamientos jurídicos que esta aclaración conste a nivel legal y no en la norma suprema. Solamente menciona, de manera genérica, que se protegen tanto los datos como la información con la condición de que sean personales. Esta norma, al haberse redactado de forma

21. Ecuador. Tribunal Constitucional (Sentencia No. 0070-2003-HD), *R. O.* 271 de 11 de febrero de 2014.

abierta y general, establece un sistema de protección del derecho la autodeterminación informativa en el que, cualquiera sea la clasificación del dato: nominativos, innominativos; reservados, secretos o públicos, notorios; sensibles o no sensibles; existenciales o no existenciales,[22] que conste en ficheros de acceso público o en ficheros de naturaleza privada, con la condición *sine qua non*, de que sean personales, esto es asociados a un titular.

ANÁLISIS DE LOS TÉRMINOS DOCUMENTOS, DATOS GENÉTICOS, BANCOS O ARCHIVOS DE DATOS PERSONALES E INFORMES EN LA GARANTÍA CONSTITUCIONAL DE HÁBEAS DATA

En Ecuador, la garantía constitucional con la que se permite el ejercicio de los denominados derechos ARCO[23] es el hábeas data contenido en el artículo 92 de la CRE.

Al respecto, es necesario analizar cada uno de los términos empleados en este artículo: documentos, datos genéticos, bancos o archivos de datos personales e informes; porque, lejos de englobar e incluir todas las formas de manifestación de un dato que puedan garantizar una protección adecuada del derecho, pueden llegar a restringir su procedencia y a causar confusión.

Sobre este tema la sentencia No. 001-14-PO-CC de 3 de julio de 2014, dictada por la Corte Constitucional ecuatoriana, anteriormente analizada, en su análisis señala:

> El problema respecto de la diferenciación entre conceptos como "documento", "archivo", "dato", "banco de datos", "información" y otros relacionados con la materia, sin duda no es estrictamente jurídico, sino que corresponde también, entre otros campos, al de la informática. Empero, las implicaciones del sentido y alcance que se dé a cada uno de los conceptos enunciados, así como a la correcta diferenciación entre ellos, deberá ser determinado a través de un ejercicio hermenéutico, y por tanto, tendrá directa relación con el contenido del derecho constitucional protegido por medio de la acción de hábeas data. Así, para la solución del caso concreto y la emisión de reglas jurisprudenciales que se deriven de los

22. Osvaldo Alfredo Gozaíni, *Habeas data: protección de datos personales. Doctrina y jurisprudencia* (Buenos Aires: Rubinzal-Culzoni, 2001).
23. Son parte del contenido clásico del derecho a la protección de datos personales: el acceso, la rectificación, la cancelación y la oposición. Con la inicial de cada uno de estos derechos se forma el acrónimo ARCO. Serrano Pérez, *El derecho fundamental a la protección de datos. Derecho español y comparado*, 343.

hechos presentados, esta Corte deberá recurrir a las fuentes doctrinarias que permitan comprender qué protege la garantía jurisdiccional en particular.[24]

La Corte Constitucional señala que es necesario analizar cada caso concreto que se presente, y en el que se invoque cada uno de los elementos enlistados en la norma, por el sentido y alcance de cada uno de estos conceptos y sus posibles consecuencias. Además, para un adecuado análisis, se deberá acudir a las fuentes doctrinarias.[25] En este sentido, a continuación se contribuye con lo siguiente:

Documento

La norma por expresa mención regula tanto documentos electrónicos como documentos físicos. Se entiende como documento físico "todo escrito legible o descifrable directamente por el ser humano y aportado normalmente en papel (o en el elemento que en cada momento histórico estaba vigente)".[26]

En cambio, el documento electrónico es "un instrumento que se confecciona por medio de elementos electrónicos y que solo puede ser leído, comunicado o transmitido con la ayuda de ciertos medios técnicos que hacen perceptibles o inteligibles las señales digitales que lo integran".[27]

La diferencia entre este tipo de documentos radica en el soporte, ya que los primeros pueden ser entendidos directamente por el ser humano o a través de ciertos medios técnicos. Empero, respecto de sus funciones y efectos jurídicos, los documentos electrónicos y documentos físicos son equiparables por aplicarse en ellos el principio de equivalencia funcional establecido en el artículo 2 de la Ley No. 67, Ley de Comercio Electrónico, firmas y mensajes de datos del Ecuador, publicado en el Registro Oficial Suplemento 557 de 17 de abril de 2002.

Es indispensable aclarar que el derecho a la protección de datos resguarda no solo datos virtuales sino también físicos, porque se protege el dato personal que ha sido informatizado y aquel que es susceptible de informatizarse,[28] como por ejemplo: un archivo o fichero con datos no tratados o incluso un fichero físico.

---

24. Ecuador. Corte Constitucional (Sentencia No. 001-2014-PJO-CC).
25. Ibíd.
26. José Antonio Vega Vega, *Derecho mercantil electrónico* (Madrid: Reus, 2015), 27. Disponible en ‹http://public.eblib.com/choice/publicfullrecord.aspx?p=4569794›.
27. Ibíd.
28. Ya que esta informatización se puede llevar a cabo incluso de forma material con la simple "[...] organización y estructura lógica de los datos en un fichero –aunque sea manual–, que permita su fácil

Nuevamente la sentencia No. 001-14-PO-CC analiza la naturaleza de los presupuestos en análisis, para concluir que no es importante la forma en la que el dato o la información se presente –sea este físico: imprimible o documentable; o virtual: registrado en soporte digital–, sino que se protege el contenido informativo. En este sentido, la jurisprudencia ecuatoriana confirma que el hábeas data opera en soporte digital o físico.[29]

Ahora bien, superada la discusión sobre la virtualidad o materialidad, el término documento ha propiciado una confusión en el foro ecuatoriano, debido a que se presentan acciones constitucionales de hábeas data cuando en realidad se pretenden iniciar, ya sea como prueba o diligencia previa, procedimientos ordinarios[30] de mera legalidad, como el de exhibición de documentos.[31]

La Corte Constitucional en sentencia No. 0044-2007 intenta solucionar esta confusión estableciendo que:

---

acceso, tratamiento y recuperación o consulta de la información". Miguel Ángel Davara Rodríguez, *Manual de derecho informático* (Cizur Menor: Thomson Aranzadi, 2015), 50.

29. Ecuador. Corte Constitucional (Sentencia No. 001-2014-PJO-CC): el "documento" funge como uno de varios medios en los que es posible impregnar o "imprimir" tal representación por medio de símbolos, a fin de lograr la preservación del dato y la información que se puede extraer de él. Por ende, no interesa para el hábeas data, como garantía, el papel y la tinta utilizados para registrar el dato, ni el disco duro en el cual se encuentre la información –denominados por el constituyente como "soporte material o electrónico" de los datos–, ni cualquier forma ideada por el ingenio humano para su preservación, sino que, como la expresión lo señala, el derecho tutelado recae sobre el dato mismo y el uso informativo que se le dé.
30. Ecuador. *Código Orgánico General de Procesos* (*COGEP*), art. 122.- Diligencias preparatorias. Además de otras de la misma naturaleza, podrá solicitarse como diligencias preparatorias: 1. La exhibición de la cosa mueble que se pretende reivindicar o sobre la que se practicará secuestro o embargo; la del testamento, cuando la o el peticionario se considere la o el heredero, legataria o legatario o albacea; la de los libros de comercio cuando corresponda y demás documentos pertenecientes al comerciante individual, la sociedad, comunidad o asociación; exhibición de los documentos necesarios para la rendición de cuentas por quien se halle legalmente obligado a rendirlas; y en general, la exhibición de documentos en los casos previstos en este Código. 2. La exhibición de los títulos u otros instrumentos referentes a la cosa vendida, por parte de su enajenante en caso de evicción o pretensiones similares. 3. El reconocimiento de un documento privado. 4. El nombramiento de tutora o tutor o curadora o curador para las o los incapaces que carezcan de guardadora o guardador o en los casos de herencia yacente, bienes de la persona ausente y de la o del deudor que se oculta. 5. La apertura de cajas o casilleros de seguridad en las instituciones del sistema financiero. 6. La inspección preparatoria si la cosa puede alterarse o perderse. 7. La recepción de las declaraciones urgentes de las personas que, por su avanzada edad o grave enfermedad se tema fundadamente puedan fallecer o de quienes estén próximos a ausentarse del país en forma permanente o por un largo período". *LEY 0*, *Registro Oficial Suplemento* No. 506 de 22 de mayo de 2015.
31. Ecuador. Corte Constitucional (Sentencia No. 0039-2008-HD), *R. O. Suplemento* 86 de 5 de diciembre de 2008.

> ...la diferencia fundamental entre la exhibición de documentos y la acción de hábeas data está dada por el tipo de información requerida y la finalidad perseguida con tal acción; para ello, debe tomarse en cuenta que no se trata de cualquier tipo de información sino aquella relacionada con información personal cuya divulgación cause perjuicio o viole su derecho a la intimidad, al honor y a la buena reputación, y que la finalidad es justamente conocer que uso se está dando a esa información, para hacer efectiva la protección de sus derechos.[32]

En tal sentido, la acción de hábeas data –a diferencia del procedimiento de exhibición de documentos– tiene por finalidad el acceso a los datos para ejercitar el derecho a la autodeterminación informativa o para la implementación de los derechos de rectificación, cancelación y anulación, cuando la información sea incorrecta, incompleta o desactualizada, todo ello con miras a evitar actos discriminatorios o perjuicios relacionados con la transgresión de otros derechos fundamentales como el honor, la intimidad y ahora la protección de datos personales.

La sentencia No. 001-14-PO-CC de 3 de julio de 2014, dictada por la Corte Constitucional ecuatoriana, señala como regla de cumplimiento obligatorio por constituir precedente jurisprudencial el que no se puede usar la acción de hábeas data para conseguir la entrega física del documento que contiene datos o información personal, sea que este se encuentre en soporte material o electrónico.[33]

Finalmente, existe una interpretación por la cual se puede entender el término *documento* como el conjunto de datos,[34] de tal forma que no se asocie este término al soporte en el que se encuentren. Esta perspectiva podría solucionar la equivocada compresión que el término documento ha tenido en nuestro país. Ante la imprecisión normativa, es a la Corte Constitucional a la que le corresponde aclarar el sentido en el que debe entenderse el término *documento* para evitar la confusión antes señalada. Además, la alusión a *documento físico o electrónico* en realidad se refiere al soporte

---

32. Ecuador. Corte Constitucional (Sentencia No. 0044-2007-HD), *R. O. Suplemento* 137 de 4 de agosto de 2009.
33. Ecuador. Corte Constitucional (Sentencia No. 001-2014-PJO-CC): 6. El hábeas data, como mecanismo de garantía del derecho a la protección de datos personales, no podrá ser incoado como medio para requerir la entrega física del soporte material o electrónico de los documentos en los que se alegue está contenida la información personal del titular sino para conocer su existencia, tener acceso a él y ejercer los actos previstos en el artículo 92 de la Constitución de la República; el juez está obligado a utilizar todos los mecanismos que establece la ley para efectos de garantizar debida y eficazmente los actos constantes en el artículo referido.
34. Davara en su texto señala que cuando "el dato o la documentación –como conjunto de datos– son sometidos a un tratamiento o adecuación a un fin, para obtener un resultado elaborado, se convierten en información". Davara Rodríguez, *Manual de derecho informático*, 53.

donde se encontrarán los datos personales, por lo que dicha referencia podría ser suprimida, y en la norma únicamente debería constar de forma genérica que se protege el acceso a datos personales físicos o virtuales y eliminar el término documento.

a) Dato genético: No se refiere a las muestras en sí mismas, ya que no pueden ser consideradas datos sino fuente de datos,[35] sino a los análisis genéticos, mapas o a informes o conclusiones que se realicen de la comprensión de dichos resultados. Al parecer, su incorporación en el texto constitucional se debe a las dudas, en varios ordenamientos jurídicos extranjeros, sobre su condición de dato personal, de tal forma que los asambleístas ecuatorianos consideraron que era indispensable su expresa mención para evitar estas discusiones o debates y garantizar una protección integral.

b) Bancos o archivos de datos personales o de sus bienes: Al respecto la cualificación de que estos datos deban pertenecer a bancos o archivos resulta además de innecesaria, impertinente, ya que establece una condición excluyente pues solo podría solicitarse hábeas data respecto de aquellos que se encuentren almacenados en un banco o archivo, cuando pueden existir datos sueltos,[36] pero evidentemente relacionados con una persona, y que por lo tanto, sean dignos de protección.

c) Informes sobre sí misma, o sobre sus bienes: El término informe[37] a efectos de establecer la procedencia del hábeas data hace referencia nuevamente al soporte el que estarán contenidos los datos personales. Pues podrán estar descritos o expuestos a través de un informe que puede constar en formato físico o si se trata de un sonido, imagen, fotografía, gráfico, entre otros, puede constar en formato electrónico. Nuevamente, resulta equivoco el uso del término *informe* ya que no se deben proteger los datos por constar en un determinado formato sino por su naturaleza.

---

35. Javier Aparicio Salom, *Estudio sobre la protección de datos* (Navarra: Aranzadi, 2013), 108.
36. Se ha pronunciado en este sentido el G29 en el Dictamen 4/2007 sobre el concepto de datos personales cuando dice: "para que la información sea considerada como datos personales no es necesario que esté recogida en una base de datos o en un fichero estructurado. También la información contenida en un texto libre, en un documento electrónico puede calificarse como datos personales, siempre que se cumplan los otros criterios de definición de datos personales". G29, "Dictamen 4/2007 sobre el concepto de datos personales", 20 de junio de 2007.
37. Respecto del término "informe", la Real Academia de la Lengua señala dos acepciones más cercanas al tema de análisis; en primer lugar, la "Descripción, oral o escrita, de las características y circunstancias de un suceso o asunto"; asimismo, dice que es la "Exposición total que hace el letrado o el fiscal ante el tribunal que ha de fallar el proceso". RAE-ASALE, "Diccionario de la Lengua Española. Edición del Tricentenario", *Diccionario de la Lengua Española*, acceso: 18 de enero de 2017. Disponible en ‹http://dle.rae.es/?id=LYB2BS5|LYF57Ax›.

CONCLUSIONES

Conforme consta en el número 19 del artículo 66 de la Constitución de la República del Ecuador, el presupuesto del derecho a la protección de datos personales es *el dato y la información de carácter personal.*

La posición jurisprudencial de carácter referencial que limita la procedencia del hábeas data a los datos informativos o con función informativa, debiera ser aplicada solo a los otros derechos protegidos por esta garantía jurisdiccional como: el honor, el buen nombre y la intimidad personal y familiar. Ya que, en el caso del derecho a la protección de datos personales, el hábeas data debe adaptarse al contenido de este derecho fundamental y resguardar no solo el dato con contenido informativo, sino también proteger al dato por sí solo, porque, aunque inicialmente carece de la característica informativa, puede ser tratado, perfilar a un individuo y afectar su autodeterminación informativa e incluso otros derechos fundamentales.

Adicionalmente, en el artículo 92 de la CRE no existe mención expresa a los términos genéricos *datos e información*. La garantía constitucional se encontraría incompleta y sería insuficiente para determinar un adecuado marco de protección porque se debe proteger el dato y la información y no solo sus manifestaciones o procesamientos, precisamente para evitar que en el avance de la tecnología existan datos que pudieran quedar fuera del régimen de protección por no calzar alguna de las expresiones constantes en la norma, esto es, documentos, datos genéticos, bancos o archivos de datos personales e informes sobre sí misma, o sobre sus bienes.

Tanto la norma que hace alusión al derecho fundamental como aquella que consagra la garantía constitucional del hábeas data deben proteger el acceso, la decisión y gestión del dato o de la información, incluidos de forma expresa los datos genéticos, en cualquier soporte físico virtual, ya sean que estos consten en documentos o informes, se encuentren de forma aislada o incorporados a archivos o bancos de datos, sean parte o no de cualquiera otra forma de recogida o procesamiento y versen sobre la persona misma o sobre sus bienes. La única condición clara y coincidente es que estos datos deben vincularse a personas identificadas o identificables, no necesariamente íntimos sino que todo tipo de dato personal incluso aquel considerado inocuo que amerita protección en virtud de su potencialidad y de los actuales avances en minería de datos y la elaboración de perfiles.

BIBLIOGRAFÍA

Aparicio Salom, Javier. *Estudio sobre la protección de datos*. Navarra: Aranzadi, 2013.

ASALE, RAE. *Diccionario de la lengua española*. Acceso: 18 de enero de 2017. Disponible en ‹http://dle.rae.es/?id=LYB2BS5|LYF57Ax›.

Conde Ortiz, Concepción. *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*. Madrid: Dykinson, 2005.

Consejo de Europa. "Recomendación No. R (97) 18 y Exposición de Motivos del Comité de Ministros a los Estados Miembros relativa a la protección de datos de carácter personal, recogidos y tratados con fines estadísticos", 30 de septiembre de 1997.

Davara Fernández de Marcos, Isabel. *Hacia la estandarización de la protección de datos personales: propuesta sobre una "Tercera Vía o Tertium Genus" Internacional*. Madrid: La Ley, 2011.

Davara Rodríguez, Miguel Ángel. *Manual de Derecho informático*. Cizur Menor: Thomson Aranzadi, 2015.

Fernández Esteban, María Luisa. *Nuevas tecnologías, internet y derechos fundamentales*. Madrid: MacGraw-Hill, 1998.

Gil, Elena. *Big Data, privacidad y protección de datos*. Madrid, Agencia Española de Protección de Datos, 2016.

Gozaíni, Osvaldo Alfredo. *Habeas Data: protección de datos personales: doctrina y jurisprudencia*. Buenos Aires: Rubinzal-Culzoni, 2001.

Pardini, Anibal. "La información y su sistema de protección". *Revista de Direito do Comércio Internacional Temas e Atualidades Internet, Comércio Eletrônico E Sociedade da Informação* (2006).

Santos García, Daniel. *Nociones generales de la Ley Orgánica de Protección de Datos y su reglamento: adaptado al RD 1720/2007 de 21 de diciembre*, 2a. ed. Madrid: Tecnos, 2012.

Troncoso Reigada, Antonio. *La protección de datos personales: en busca del equilibrio*. Valencia: Tirant lo Blanch, 2010.

Vega Vega, José Antonio. *Derecho mercantil electrónico*. Madrid: Reus, 2015. Disponible en ‹http://public.eblib.com/choice/publicfullrecord.aspx?p=4569794›.

Zabía de la Mata, Juan, e Irene Ma. Agúndez Lería, edit. *Protección de datos: comentarios al reglamento*. Valladolid: Lex Nova, 2008.

Otros

Corte Constitucional del Ecuador. "Sentencia No. 001-2014-PJO-CC". *Gaceta Constitucional* No. 007, 3 de julio de 2014.

---. "Sentencia No. 0039-2008-HD", n.d. *R. O. Suplemento* 86, 5 de diciembre de 2008.

---. "Sentencia No. 0044-2007-HD", 21 de mayo de 2009. *R. O. Suplemento* 137, 4 de agosto de 2009.

G29. "Dictamen 4/2007 Sobre El Concepto de Datos Personales", 20 de junio de 2007.

Tribunal Constitucional del Ecuador. "Sentencia No. 0070-2003-HD". *R. O.* 271, 11 de febrero de 2004.

Fecha de recepción: 13 de marzo de 2017
Fecha de aprobación: 15 de mayo de 2017

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración

*Luis Ordóñez Pineda**

RESUMEN

En las últimas décadas del siglo XX se ha reconocido la existencia de un derecho fundamental a la protección de datos personales, tanto en los tratados y acuerdos internacionales como en las Constituciones de distintos países, lo que se ha traducido en un desarrollo legislativo de este derecho fundamental tendiente a regular el tratamiento de la información personal tanto en el ámbito público como privado. En el caso de Ecuador, el surgimiento del derecho a la autodeterminación informativa se enmarca en los principios consagrados dentro de la teoría del neoconstitucionalismo andino, enmarcados fundamentalmente en la democracia participativa y en la constitucionalización de nuevos derechos fundamentales. Esta investigación está orientada a estudiar –en el contexto de la Comunidad Andina– los precedentes constitucionales, jurisprudenciales y doctrinarios que enmarcan el origen y desarrollo de este derecho fundamental. A partir de la experiencia europea, este análisis pretende promover un modelo interamericano de integración para una regulación equilibrada respecto al tratamiento de los datos personal.

Palabras clave: Derecho a la autodeterminación informativa, hábeas data, garantías constitucionales, Derecho a la intimidad, Comunidad Andina, Derecho comparado, Integración Interamericana.

ABSTRACT

During the 20th century and especially in the last decades there has been an important recognition of the personal data protection as a fundamental right, both in the International Treaties and Agreements and in the Constitutions of different countries. This has resulted in a legislative development of fundamental rights in order to regulate the treatment of personal information both in public and private sector. In Ecuador, the emergence of the right to informational self-determination is framed within the principles preserved in the Andean Neo Constitutionalism

* Docente-investigador, departamento de Ciencias Jurídicas, Universidad Técnica Particular de Loja.

stated in participatory democracy and in the Constitutionalism of new fundamental rights, fundamentally. This research is aimed at studying –in the context of the Andean Community– the constitutional, jurisprudential and doctrinal precedents that frame the origin and development of this fundamental right. Based on the European experience, this analysis aims to initiate an Interamerican Model of Integration for a balanced regulation respect to the processing of the personal data.

KEYWORDS: Right to informational self-determination, Hábeas data, Constitutional guarantees, right to privacy, Andean Community, Comparative law, Interamerican Integration.

FORO

INTRODUCCIÓN

Con la evolución de la tecnología, la sociedad ha experimentado gran dificultad para mantener protegidos algunos bienes jurídicos tradicionalmente tutelados a través del derecho a la intimidad, que ahora requieren una tutela más específica y amplia que les proporciona el derecho a la protección de datos personales o la autodeterminación informativa.[1] Como se sabe, existen varias problemáticas derivadas de los avances tecnológicos, que se traducen en necesidades al momento de garantizar este derecho fundamental a partir del tratamiento de la información, sea en el ámbito público o privado.

Pablo Lucas Murillo asegura que "la potencialidad de la tecnología ha llegado a tal punto que permite obtener resultados socialmente provechosos. El problema es que, de igual modo, resulta idónea para causar perjuicios de entidad semejante a los beneficios".[2]

1. Según Pablo Lucas Murillo, la expresión "autodeterminación informativa" o "intimidad informativa" puede ser considerada como "más expresiva" que otras adoptadas por los legisladores y la doctrina para hacer referencia al derecho fundamental a la protección de datos de carácter personal. Cabe señalar que más adelante nos referiremos de manera pormenorizada sobre el contenido de esta expresión.
2. Pablo Murillo de la Cueva y José Luis Piñar, *El derecho a la autodeterminación informativa* (Madrid-México: Fontamara, 2011), 16. Precisamente, el marco común en los países de la Comunidad Andina son los problemas derivados de la protección de las libertades fundamentales a partir del uso de las tecnologías y como resultado de la evolución del paradigma del tratamiento de la información desde medios impresos hacia la digitalización de la información personal.

En los estados democráticos de la Comunidad Andina (CAN),[3] el proceso de constitucionalización de los derechos fundamentales de las personas incorporó recientemente como derecho autónomo la protección de datos personales frente a la necesidad de dar respuesta al proceso de evolución tecnológica.

Por otra parte, Hassmer y Chirino señalan que "el desarrollo del derecho a una protección de datos personales se alimenta en las sociedades modernas de dos fuentes: de la tempestuosa marcha triunfal de la tecnología de la información, en conjunto con el escepticismo sobre el Estado y lo que de este puede esperarse".[4] En el contexto latinoamericano la protección de datos personales se ha derivado de la necesidad de salvaguardar los derechos o libertades personales que pueden ser afectadas en virtud del tratamiento de la información personal, principalmente, derivada de la incorporación de procesos tecnológicos en el tratamiento de la información.

Inicialmente, algunas reformas constitucionales en la CAN "introdujeron la protección de los datos personales (algunas bajo la forma de hábeas data), viz. Brasil (1998) art. 5o.- X, XII y LXXII; art. 105 l b); Colombia (1991) art. 15; Paraguay (1992) art. 33, 36 y 135; Perú (1993) art. 2o., 162, 203-3; Argentina (1994) art. 19 y 43; y Ecuador (1998) art. 23.8, 23.13, 23.24, 94".[5] En el caso de Ecuador, en el año 1998 la protección de datos de carácter personal no se hallaba reconocida como un derecho fundamental, y, más bien, sus facultades se ejercían a través de otros derechos civiles como la intimidad personal y familiar, entre otros; y al hábeas data como garantía constitucional.

En la actualidad, el derecho a la protección de los datos de carácter personal se describe como un derecho autónomo de otros derechos, es decir, como un derecho nuevo vinculado a la necesidad de proteger la dignidad personal frente a las nuevas tecnologías.[6] Por consiguiente, este nuevo derecho fundamental constituye "un *instituto*

---

3. La Comunidad Andina actualmente está conformada por cuatro países miembros: Bolivia, Colombia, Ecuador y Perú; cinco países asociados: Chile, Argentina, Brasil, Paraguay y Uruguay; y, un país observador: España.
4. Winfried Hassmer y Alfredo Chirino Sánchez, *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales* (Buenos Aires: Editores del Puerto, 1997), 28.
5. Carlos Gregorio, "Protección de datos personales: Europa *vs.* Estados Unidos, todo un dilema para América Latina", en Raúl Márquez Romero, coord., *Transparentar al Estado: la experiencia mexicana de acceso a la información* (México: Instituto de Investigaciones Jurídicas, 2005), 310-1.
6. En este contexto, "de las iniciales elaboraciones teóricas que buscaban extender los confines del derecho a la intimidad a toda información personal, se pasó a identificar un bien jurídico autónomo, denominado intimidad informativa, *privacy*, libertad informática o autodeterminación informativa". Cfr. Murillo de la Cueva y Piñar, *El derecho a la autodeterminación informativa*, 17. En breves términos, la consolidación de la protección de datos personales como un derecho fundamental ha

de garantía de otros derechos fundamentales, en especial del derecho a la intimidad, pero no solo de este derecho... Atribuye a su titular un haz de facultades que consiste en el poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos".[7]

Con estos antecedentes, este artículo se plantea recorrer el reconocimiento constitucional del derecho fundamental a la protección de datos personales en los ordenamientos jurídicos de los países miembros de la CAN –con especial énfasis a su incorporación en Ecuador–, además de los que la conforman en calidad de países asociados y observador. Al final, el corolario de este análisis supone una idea base de un modelo interamericano de integración que –con base en la experiencia europea y en los avances generados por el Comité Jurídico Interamericano y Departamento de Derecho Internacional de la Organización de Estados Americanos– sirva de paradigma para la regulación del derecho a la autodeterminación informativa en las Américas.

RECONOCIMIENTO CONSTITUCIONAL DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN LA COMUNIDAD ANDINA. HACIA UN MODELO INTERAMERICANO DE INTEGRACIÓN

Antecedentes

En general, la constitucionalización de los derechos no ha sido una tarea muy fácil dentro de los sistemas jurídicos. En el caso del derecho fundamental a la autodeterminación informativa se originó a partir del debate que consideraba el derecho a la intimidad como insuficiente para proteger de manera integral a la persona frente a los avances tecnológicos.

Gran parte del mérito sobre su constitucionalización, aunque no suficiente, han tenido las declaraciones regionales en materia de derechos humanos. En la CAN ha sido la Convención Americana sobre Derechos Humanos (CADH).[8] La principal caracte-

---

transitado desde la necesidad de proteger el tratamiento de la información frente a los avances tecnológicos hasta su separación –teórica y jurídica del derecho a la intimidad– y posterior reconocimiento constitucional como un derecho fundamental relacionado con el control y acceso de la información personal.

7. Antonio Troncoso, *La protección de datos personales: en busca del equilibrio* (Valencia: Tirant lo Blanch, 2010), 69.
8. La Convención Americana sobre Derechos Humanos fue suscrita en la Conferencia Especializada

rística de esta declaración es el intento de proteger el tratamiento de datos personales a través de la intimidad personal y familiar. Por consiguiente, la CADH[9] puede significar el instrumento regional más importante para la derivación del derecho a la protección de datos personales afianzado en el derecho a la intimidad personal y familiar.

A esta protección se suma que en 2012 el Comité Jurídico Interamericano (CJI) de la Organización de Estados Americanos (OEA) presentó la "Propuesta de declaración de principios de Privacidad y Protección de Datos Personales en las Américas"[10] contenida en doce principios[11] relativos a la protección sobre el tratamiento impropio de la información personal. Dicha propuesta se consolidó en marzo de 2015, cuando el CJI adoptó[12] el informe formulado por David P. Stewart sobre los "Principios para la

---

Interamericana sobre Derechos Humanos el 22 de noviembre de 1969, en San José de Costa Rica. Adicionalmente, puede considerarse: la Decisión 439, del 17 de junio de 1998, sobre el Marco General de Principios y Normas para la Liberalización del Comercio de Servicios en la Comunidad Andina (art. 11) para la aplicación de medidas relativas a la protección de la intimidad en relación con el tratamiento y la difusión de datos personales; la Carta Andina para la Promoción y Protección de los Derechos Humanos, del 26 de julio de 2002, (art. 20) sobre el acceso del individuo a la información sobre su persona; el Acuerdo de Diálogo Político y Colaboración, del 15 de octubre de 2003, entre la Comunidad Europea y la Comunidad Andina (art. 35 y 58) sobre cooperación en materia de protección de datos; la 6383 de la Comunidad Andina, del 21 de julio de 2006, sobre lineamientos comunitarios de protección del usuario y en el cual se incluye (art. 2) el mantenimiento de reserva de los datos personales derivados del uso de las telecomunicaciones; la Tercera Ronda de negociaciones entre la CAN y la UE, del 21-25 de abril de 2008, en temas vinculados a la protección de datos personales.

9. Los números 2 y 3 del artículo 11 de la Convención Americana refieren, respectivamente: "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".
10. En el 80 período ordinario de sesiones del Comité Jurídico Interamericano, la propuesta fue aprobada por unanimidad mediante la resolución CJI/RES. 186 (LXXX-O/12) en sesión celebrada el 9 de marzo de 2012.
11. Los doce principios adoptados por el Comité Jurídico Interamericano, en su orden, son: Propósitos legítimos y justos; Claridad y consentimiento; Pertinencia y necesidad; Uso limitado y retención; Deber de confidencialidad; Protección y seguridad; Fidelidad de la información; Acceso y corrección; Información sensible; Responsabilidad; Flujo transfronterizo de la información y responsabilidad; y, Publicidad de las excepciones.
12. En el 86 período ordinario de sesiones del Comité Jurídico Interamericano, en sesiones celebradas en marzo de 2015, se adopta por consenso la denominada guía legislativa para los Estados Miembros fundamentada en los doce principios aprobados en 2012. Cabe señalar que se introdujeron cambios en los principios siete, nueve y once; lo más significativo ha sido la sustitución del término "información" por el de "datos". La finalidad de esta guía legislativa es encaminar a los Estados Miembros en la formulación de leyes nacionales y normas relativas a la protección del derecho a la autodeterminación informativa teniendo como base una Ley Interamericana.

Privacidad y la Protección de Datos Personales" que consiste en la fundamentación de los doce principios aprobados en 2012. Adicionalmente, el Departamento de Derecho Internacional (DDI) de la OEA ha presentado una compilación de documentos básicos que pueden servir para el proceso de elaboración de una "Ley Modelo Interamericana sobre protección de datos personales".[13]

Para consolidar este objetivo, la Corte Interamericana de Derechos Humanos (CIDH)[14] se presenta como un órgano de promoción y protección en el ámbito de la CADH. Los precedentes jurisprudenciales que la Corte ha resuelto sobre el derecho fundamental a la protección de datos personales han sido progresivos y conexos a la vida privada, intentando asignar su debida garantía. Por ejemplo, la CIDH ha definido que:

> El art. 11.2 de la Convención protege la vida privada y el domicilio de injerencias arbitrarias o abusivas. Dicho artículo reconoce que existe un ámbito personal que debe estar a salvo de intromisiones por parte de extraños y que el honor personal y familiar, así como el domicilio, deben estar protegidos ante tales interferencias. La Corte considera que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública.[15]

---

13. La compilación presentada por el Departamento de Derecho Internacional, para el fin de elaboración de una "Ley Modelo Interamericana sobre protección de datos personales", se compone de cinco apartados: a) Glosario Iberoamericano de Protección de Datos Personales; b) Estudio comparativo de la legislación en materia de protección de datos personales en Latinoamérica; c) Sistemas de Protección de Datos Personales (APEC y Unión Europea); d) Resoluciones, declaraciones, acuerdos y directrices internacionales; y, e) Aportes del Centro de Protección de Datos Personales (CPDP) de la Ciudad Autónoma de Buenos Aires, Argentina, y una opinión técnica del Instituto Federal de Acceso a la información y Protección de Datos (IFAI) de México.
14. Sobre la base de lo dispuesto en la Convención Americana de Derechos Humanos, la Corte Interamericana es competente para conocer de los asuntos relacionados con el cumplimiento de los compromisos contraídos por los Estados Partes en la Convención; es decir: "Los Estados Partes en esta Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna" (artículo 1 de la Convención Americana de Derechos Humanos).
15. Cfr. Caso de las Masacres de Ituango *vs.* Colombia, Sentencia de 1 de julio de 2006. Serie C No. 148. párr. 193 y 194. Sobre esta base, la Corte Interamericana ha señalado que la Convención Americana: "protege la confidencialidad e inviolabilidad de las comunicaciones frente a cualquier injerencia arbitraria o abusiva por parte del Estado o de particulares, razón por la cual tanto la vigilancia como la intervención, la grabación y la divulgación de esas comunicaciones quedan prohibidas, salvo en los casos previstos en ley y que se adecuen a los propósitos y objetivos de la Convención Americana. Cfr. Caso Escher y otros *vs.* Brasil, de 6 de julio de 2009. Serie C No. 200.

Asimismo, en relación a los bienes jurídicos tutelados, la CIDH sostiene que "la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás".[16] Por tanto, la protección a la vida privada incluye una serie de factores relacionados con la dignidad humana, tales como:

> la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales [...] engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior.[17]

Mientras que lo más cercano a una definición adecuada se recogen en dos fallos. El primero, relacionado al manejo de bases de datos sobre personas desaparecidas, conceptualizándose como una "garantía de no repetición" que "en todo momento deberá proteger los datos personales contenidos en dichas bases de datos";[18] y el segundo que hace referencia al derecho a la identidad como "el conjunto de atributos y características que permiten la individualización de la persona en sociedad".[19]

---

16. Cfr. Caso Atala Riffo y niñas *vs.* Chile. Sentencia de 24 de febrero de 2012 Serie C No. 239, párr. 162. A esta importante consideración, la Corte –citando al Tribunal Europeo de Derechos Humanos– señala que "el derecho a la vida privada abarca la identidad física y social, el desarrollo personal y la autonomía personal de una persona". Cfr. párr. 135, supra nota 158, Caso Pretty *vs.* Reino Unido (No. 2346/2), Sentencia de 29 de abril de 2002.
17. Cfr. Caso Artavia Murillo y otros *vs.* Costa Rica. Sentencia de 28 de noviembre de 2012 Serie C No. 257, párr. 143. Sobre esta consideración, la Corte –citando al Tribunal Europeo de Derechos Humanos– señala que "La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona". Cfr. párr. 143, supra nota 228, Caso R.R. *vs.* Polonia (No. 27617/04), Sentencia del 26 de mayo de 2011.
18. Cfr. Caso González y otras *vs.* México. Sentencia de 16 de noviembre de 2009 Serie C No. 205, párr. 512.
19. Cfr. Caso Gelman *vs.* Uruguay. Sentencia de 24 de febrero de 2011 Serie C No. 221, párr. 122. En esta parte, es preciso acotar que la resolución adoptada en marzo de 2015 por el CJI, define a los datos personales considerando que: "Tal como se usa en estos principios, la frase "datos personales" abarca la información que identifica o puede usarse de manera razonable para identificar a una persona en particular de forma directa o indirecta". En este contexto, cfr. Las Hermanas Serrano Cruz *vs.* El Salvador. Sentencia de 1 de marzo de 2005 Serie C No. 120, párr. 138, la Corte Interamericana ha señalado que "el derecho a la identidad presupone el libre conocimiento de datos personales y familiares, y acceso a estos, para satisfacer a una necesidad existencial y salvaguardar los derechos individuales. Dicho derecho tiene además un notorio contenido cultural (además de social, familiar, psicológico, espiritual), mostrándose esencial para la relación de cada persona con las demás e incluso su comprensión del mundo exterior, y su ubicación en el mismo".

Bajo esta realidad, y con las excepciones que se verán más adelante –a diferencia de los países de la CAN–, en sistemas jurídicos comparados como la Unión Europea la evolución del derecho a la autodeterminación informativa ha tenido mayor desarrollo. En concreto, como menciona Murillo de la Cueva, el afianzamiento de la tutela de este derecho en la Comunidad Europea ha surgido de la búsqueda de un modelo común a partir de "una suerte de diálogo entre la doctrina, los legisladores internacional, comunitario y estatal y la jurisprudencia".[20]

En efecto, a nivel comunitario destacan el Tratado de Lisboa, la Carta de los Derechos Fundamentales de la Unión Europea, el Convenio 108 del Consejo de Europa y el Convenio Europeo de Derechos Humanos. Sobre esta base, los principales instrumentos legislativos desarrollados son las Directivas 95/46 y 2002/58, Reglamento (CE) 45/2001 y Decisión Marco 2008/977 del Consejo orientados a enmarcar la protección de datos personales bajo un régimen de principios jurídicos comunes en la Comunidad Europea.[21]

Para el caso, en calidad de país observador de la CAN, es necesario citar la situación de España. Precisamente, sobre la base de los instrumentos comunitarios citados, en el ámbito constitucional la protección en materia de datos personales se expresa como una categoría de "derecho fundamental y libertad pública".[22] Asimismo, cuenta con una Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) y su Reglamento (RLOPD).[23] Y en relación a la actividad de supervisión y control, se destaca la actividad que desempeña la Agencia Española de Protección de Datos (AEPD) como la institución que se encarga de cumplir con los objetivos de la normativa para la protección de datos personales.

---

20. Murillo y Piñar, *El derecho a la autodeterminación informativa*, 17. Así, por ejemplo, en lo que refiere a la regulación en los países de la UE, Portugal (1976) fue el primer Estado europeo en contemplar de manera específica la protección de datos personales; le sigue, el Reino de los Países Bajos (1983), Finlandia (1919), Suecia (1994); mientras que Italia y Alemania han configurado la protección de este derecho en virtud de la jurisprudencia desarrollada por los Tribunales Constitucionales. Cfr. Troncoso, *La protección de datos personales: en busca del equilibrio*, 49-50.
21. Conviene subrayar que en la actualidad se encuentra aprobado el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo para la protección de datos personales y por el cual se derogan algunos de los instrumentos mencionados como la Directiva 95/46.
22. Algunos derechos que se desprenden del art. 18.4 de la Constitución de España son: "el derecho al honor, a la intimidad personal y familiar y a la propia imagen" y que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".
23. En todo caso, con la aprobación del Reglamento 2016/679, habrá que considerar que la normativa española y de los países comunitarios europeos cambiará de manera que se prevean las nuevas disposiciones del Reglamento (UE) 2016/679 hasta antes de 25 de mayo de 2018, fecha en la entra en vigencia.

Con estos antecedentes, a continuación se realizará una exégesis del reconocimiento constitucional, sectorial, jurisprudencial y doctrinario del derecho a la autodeterminación informativa en los países de la CAN considerando la evolución de su regulación desde el derecho a la intimidad y garantía del hábeas data hasta su configuración como un derecho de carácter fundamental. En algunos casos se observará el desarrollo de este derecho en leyes generales que han permitido efectivizar su regulación a partir de la incorporación de un modelo común con base a estándares internacionales que provienen –especialmente– del modelo europeo.

Desarrollo en las Constituciones de los países de la Comunidad Andina

La Constitución de Brasil adoptó el hábeas data como un recurso para garantizar la protección de las informaciones privadas relativas a la persona. Como señala Danilo Doneda:

> La información personal es, casi por reflejo vinculado a la privacidad mediante una simple ecuación básica que asocia un mayor grado de privacidad a la menor de la información personal y viceversa. Esta ecuación al momento de la terminación de todos los complejos problemas que rodean a esta relación, puede servir como un punto de partida para ilustrar cómo la protección de la información personal vino a buscar refugio en nuestro sistema legal: como una rama de la protección del derecho a la privacidad.[24]

Es el apartado X y LXXII del artículo 5 de la Constitución que protege la información personal, en derechos como la intimidad, la vida privada etc., y el hábeas data como una garantía sobre el acceso a las informaciones relativas a la persona bajo la protección de los derechos de la inviolabilidad de la intimidad y la vida privada.[25]

En el caso de Colombia, el artículo 15 de la Constitución advierte la protección de datos personales a través del derecho a la intimidad personal y buen nombre; así como también a través del derecho de conocer, actualizar y rectificar la información. Sobre esta base de libertades y demás garantías reconocidas en la Constitución, "el

---

24. Danilo Doneda, "A proteção dos dados pessoais como direito fundamental no direito brasileiro", *Revista Latinoamericana de Protección de Datos Personales*, No. 1 (2012).
25. Pese a considerarse como el primer país en introducir la acción de hábeas data en 1988, el desarrollo de la protección de la información personal se ha contextualizado más bien desde el derecho a la privacidad. Cfr. Danilo Doneda, "O habeas data no ordenamento brasileiro e a proteção de dados pessoais: uma integração ausente", *Revista de Derecho Comunicaciones y Nuevas Tecnologías*, No. 3 (2007).

constituyente definió la protección de la intimidad de la persona, cuando ella es fuente de información personalísima y cuando esa información se encuentra en los llamados bancos de datos, públicos o privados".[26]

La Constitución Nacional de Paraguay no contempla un derecho específico. Su protección se precisa en el derecho a la intimidad y garantía del hábeas data consagrados en los artículos 33 y 135, respectivamente. Al respecto, la doctrina considera que el hábeas data está orientado a:

> Garantizar el acceso a las informaciones y datos sobre sí misma o sobre su patrimonio que se encuentren en registros oficiales o privados de público acceso. Así mismo, toda persona está legitimada para conocer el empleo o los fines de esas informaciones y datos, así como para solicitar ante el juez competente, en caso de error o cuando se viole un derecho de la persona, su actualización, corrección o destrucción.[27]

La Constitución Política de Chile tampoco contempla un derecho fundamental y, además, del hábeas data desde el nivel constitucional. De tal suerte que, la protección de este derecho se considera sobre la base del derecho a la vida privada consagrado en el numeral 4 del artículo 19. Como señala Renato Jijena, urgen reformas en el ámbito constitucional para determinar un derecho de carácter autónomo así como constitucionalizar el hábeas data y considerar una autoridad autónoma que ejerza su protección.[28] Para este fin, en 2014 se presentó un proyecto de reforma constitucional[29] que a la

---

26. Luis Freddyur Tovar, "Positivación y protección de los derechos humanos: aproximación colombiana", *Revista Criterio Jurídico*, No. 2 (2008): 45-72.
27. Norbert Losing, "La justicia constitucional en Paraguay y Uruguay", *Anuario de Derecho Constitucional Latinoamericano*, No. 1 (2002): 109-33.
28. En concreto Jijena ha propuesto la siguiente reforma: Artículo único: Modifícase el artículo 19 número 4 de la Constitución [...] agregándose los siguientes incisos segundo y tercero: Toda persona tiene derecho a la protección de sus datos personales, los que deben ser tratados para fines concretos y específicos, con su propio consentimiento, o en virtud de otro fundamento contemplado en la ley, y tendrá, asimismo, derecho a acceder a dichos datos, para obtener su rectificación, actualización o cancelación, según procediere. Una ley orgánica constitucional establecerá las normas para la debida aplicación de este derecho, como asimismo el órgano autónomo que velará por el cumplimiento de dicha ley y controlará su aplicación. Cfr. Renato Jijena, "Tratamiento de datos personales en el Estado y acceso a la información pública", *Revista Chilena de Derecho y Tecnología*, No. 2 (2013): 49-94.
29. El artículo único del proyecto de reforma constitucional, No. 9384-07 de Senado, de 11 de junio de 2014, expresa lo siguiente: "Modifícase el artículo 19 No. 4 de la Constitución Política de la República, agregándose los siguientes incisos segundo y tercero nuevos: "Toda persona tiene derecho a la protección de sus datos personales y obtener su rectificación, complementación y cancelación, si estos fueren erróneos o afectaren sus derechos, como asimismo a manifestar su oposición, de acuer-

fecha se mantiene en etapa de tramitación. El texto incluye, precisamente, la modificación del numeral 4 del artículo 19 de la Constitución.

En el caso de Bolivia, el número 2 del artículo 21 de la Constitución protege los datos personales a través del derecho a la privacidad e intimidad; y complementariamente, según lo dispuesto en el artículo 130 mediante la acción de protección de privacidad. Sobre esta base, la acción de privacidad "conocida en el mundo jurídico como hábeas data, es una acción que protege los datos personales (edad, sexo, enfermedad, pertenencia política, etc.) de cada quien y que figuran en centros de identificación, registro electoral, registros médicos, sistemas bancarios, etc. Estos datos son de propiedad exclusiva de su titular".[30]

Derivación en el ámbito sectorial del tratamiento de información de carácter personal

Al no contemplarse en la Constitución Federal de Brasil la protección de datos personales como un derecho fundamental, su protección se desarrolla mediante leyes sectoriales como la Ley No. 9296[31] y Ley No. 9507[32] que aprueba el procedimiento del hábeas data.

En el caso de Colombia, la Ley 1266[33] desarrolla las disposiciones generales del hábeas data. Esta Ley se considera como una garantía que "refiere a la protección y

---

do con las disposiciones establecidas en la ley. Su tratamiento solo podrá hacerse por ley o con el consentimiento expreso del titular".

30. Idón Chivi, *Nueva Constitución Política del Estado: conceptos fundamentales para su desarrollo normativo, glosario de la Nueva Constitución Política del Estado* (La Paz: Vicepresidencia del Estado Plurinacional, 2010), 208.
31. La Ley No. 9296, de 24 de julio de 1996, está orientada a proteger el derecho a la privacidad de las comunicaciones. El párrafo único del artículo 1 menciona que: "Las disposiciones de la presente Ley se aplica a la interceptación del flujo de las comunicaciones de los sistemas de información y la telemática".
32. La Ley No. 9507, de 12 de noviembre de 1997, tiene por objeto regular el tratamiento de la información personal precisando las reglas sobre el derecho de acceso a la información y el procedimiento judicial de hábeas data. El artículo 7 de esta Ley refiere que el hábeas data tiene por objeto: "I.- Asegurar el conocimiento de informaciones relativas a la persona del peticionario, contenida registro o base de datos de entidades gubernamentales o de las entidades públicas". Es conveniente señalar que en la actualidad se ha presentado ante la Cámara de Diputados el Proyecto de Ley 5276/2016 que dispone considerar al tratamiento de datos personales como una garantía de libre desarrollo de la personalidad y dignidad de las personas naturales.
33. La Ley 1266 de 2008, sobre "hábeas data y manejo de la información contenida en bases de datos personales", señala en su artículo 1 que: "La presente ley tiene por objeto desarrollar el derecho

respeto del derecho a la autodeterminación informativa que contiene la intimidad e idoneidad personal que surge de la información suministrada por esta, según se deduce de lo consagrado en el artículo 15 de la Carta Política".[34] Asimismo, se destaca la Ley Estatutaria 1581[35] destinada a establecer disposiciones generales para la protección de datos personales. Es importante señalar que Colombia cuenta con el reconocimiento internacional de su autoridad de protección de datos personales[36] otorgada por la "Conferencia Internacional de Comisionados de Protección de Datos y Privacidad".[37]

Por su parte, en Paraguay la Ley No. 1682/01[38] se orienta a proteger y garantizar el ejercicio de los derechos fundamentales de los titulares de la información. Si bien es cierto, la jurisprudencia ha definido el contenido del derecho a la autodeterminación informativa y hábeas data; en un estudio realizado por la Corte Suprema se estima

---

constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política".

34. Luis Freddyur Tovar, "Positivación y protección de los derechos humanos: aproximación colombiana", 45-72.
35. La Ley Estatutaria 1581, por la cual se dictan disposiciones generales para la protección de datos personales, entró en vigencia el 17 de octubre de 2012 mediante publicación en el *Diario Oficial* 48587. El ámbito de aplicación de la Ley, según el artículo 2, señala que: "Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada".
36. El artículo 19 de la Ley Estatutaria 1581 señala que la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales ejercerá las funciones de autoridad de protección de datos personales. A este reconocimiento internacional se suma que esta autoridad, en noviembre de 2016, ha sido llamada a integrar el Comité Ejecutivo de la Red Iberoamericana de Protección de Datos Personales (RIPD).
37. La Conferencia Internacional constituye un foro de encuentro, intercambio y discusión. Es una entidad por propio derecho que representa a los miembros acreditados. La condición de miembro de la Conferencia exige que las autoridades de control y supervisión cumplan una serie de requisitos, entre los que se incluyen: a) Constituir una entidad pública creada mediante instrumento legal; b) Tener supervisión de normas específicas de protección de datos; c) Que la legislación sea compatible con los instrumentos internacionales para la protección de datos; d) Disponer de facultades legales para ejercer sus funciones; y, e) Contar con autonomía e independencia en el ejercicio de sus funciones. Cfr. Agencia Española de Protección de Datos. Disponible en ‹http://www.agpd.es/portalwebAGPD/internacional/Conferencias_inter/index-ides-idphp.php›.
38. El artículo 1 de la Ley No. 1682/01 refiere: "Esta Ley 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".

que, entre otras carencias "el nivel de protección que ofrece la legislación nacional –Ley No. 1682/2001 y Ley No. 1969/2002– es insuficiente, a efectos de que Paraguay se acredite como nación "adecuada" ante los organismos de la Unión Europea".[39]

En el caso de Chile, a partir del panorama incierto en la Constitución, la protección de este derecho se ha fortalecido sobre la garantía del hábeas data prevista en la Ley No. 19628[40] sobre la protección de la vida privada.

Finalmente, en Bolivia la Ley No. 164 se destina a proteger las telecomunicaciones y tecnologías de la información y la comunicación.[41]

Definiciones del contenido del derecho fundamental a la autodeterminación informativa en la jurisprudencia

El Supremo Tribunal Federal de Brasil mediante resolución 103236 ha señalado que:

---

39. Víctor Manuel Núñez, *Protección de datos personales* (Asunción: Centro Internacional de Estudios Judiciales, 2010), XII.
40. El artículo 1 de la Ley 19628 sobre protección de datos de carácter personal refiere que: "El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley [...] Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce". Se puede decir que esta ley llega a materializar la protección de los derechos fundamentales de los titulares de la información como resultado del tratamiento de datos personales y que se ejecuta mediante el procedimiento especial de hábeas data como lo prevé su artículo 23. Esta Ley, al considerarse como la primera en América Latina, contempla la regulación del tratamiento de la información de carácter personal en el ámbito público y privado. Cfr. Pablo Palazzi, "Avances en la protección de datos personales en América Latina", *Revista Latinoamericana de Protección de Datos Personales*, No. 3 (2011).
41. La Ley No. 164 de 2011 garantiza el "derecho humano individual" a través del aseguramiento de la protección de datos personales desde el contexto tecnológico. El artículo 59 de esta Ley expresa como obligación de los proveedores y operadores: "Brindar protección sobre los datos personales evitando la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley". Asimismo, esta Ley menciona que para los fines de procedimiento relativos al tratamiento de los datos personales, sus definiciones y principios se instrumentará un Reglamento. Precisamente, la reglamentación de esta Ley, mediante Decreto Supremo No. 1793, ha sido trascendental por cuanto desarrolla definiciones sobre el contenido del derecho a la protección de datos personales.

> La Ley 9296/1996 no hizo más que establecer directrices para resolver los conflictos entre la privacidad y la obligación del Estado de hacer cumplir las leyes penales. A pesar del carácter excepcional de la medida, el artículo XII posibilita, expresamente, una vez cumplidos los requisitos constitucionales, la interceptación de las comunicaciones telefónicas. Y tal permiso existe, por el simple hecho de que los derechos y garantías constitucionales no pueden servir de manto protector a prácticas ilícitas.

Asimismo, este Tribunal mediante resolución 673707 considera que:

> 4. El carácter público de todo registro o base de datos que contiene información que sea o puedan ser transmitidas a terceros y que no sea de uso privativo de un organismo o entidad productora o depositaria de información es inequívoco. (art. 1, Ley No. 9507/97). 5. El registro de datos debe ser entendido en su sentido más amplio, abarcando todo lo que diga respecto al interesado, sea de modo directo o indirecto (...) 6. Para interpretación el Hábeas Data extiéndase a personas físicas y jurídicas, nacionales y extranjeras, por cuanto es garantía constitucional de los derechos individuales y colectivos.

En este contexto, Brasil contextualiza la protección de los datos personales en el derecho a la intimidad en las comunicaciones, y mediante el hábeas data como acción de control constitucional. A pesar de que el derecho a la autodeterminación informativa no tiene asignación en la Constitución, puede considerarse que "el dato positivo es que no puede afirmarse que el ordenamiento brasileño este completamente al margen de estos matices".[42]

Asimismo, la Corte Constitucional de Colombia en la Sentencia de Tutela No. 175/95 expone que:

> El derecho al hábeas data, consagrado en el artículo 15 de la C P, constituye un derecho fundamental claramente diferenciado del derecho a la intimidad y el buen nombre. La jurisprudencia constitucional ha delimitado el alcance del derecho al hábeas data: ¿Cuál es el núcleo esencial del hábeas data? A juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica.

En otro fallo, la misma Corte en la Sentencia de Inconstitucionalidad No. 336/07 señala que:

---

42. Regina Linden y Temis Limberger, "Banco de datos de informaciones genéticas y la administración pública como concretizadora de la protección de datos personales y de la dignidad humana", en José Luis Barzallo, coord., *Memorias XVI Congreso Iberoamericano de Derecho e Informática* (Quito: Ministerio de Justicia, Derechos Humanos y Cultos, 2012), 261.

> En cuanto al derecho fundamental al hábeas data o a la autodeterminación informática, en diversas oportunidades la jurisprudencia de esta Corporación se ha referido a la naturaleza fundamental de este derecho, el cual comporta un plexo de facultades tales como la de disponer de la información sobre sí mismo, la de preservar la propia identidad informática, es decir, permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás.

El desarrollo teórico y práctico en Colombia, para la regulación del derecho a la autodeterminación informativa, es importante ya que cuenta con la protección en el ámbito constitucional, sectorial e institucional orientado a materializar la tutela de este derecho.

Por otra parte, la Corte Suprema de Paraguay, mediante Acuerdo y Sentencia No. 5, sobre el derecho a la autodeterminación informativa, expone que:

> El objeto de esta Institución es la persona (en su fuero íntimo, en su ámbito privado) y sus bienes (entendido como reserva y completitud), los ciudadanos debemos conocer el uso y destino dado a la información o dato sobre nuestras personas y bienes. Esto nos permite, a través de la garantía constitucional, solicitar ante el órgano judicial competente la ACTUALIZACIÓN, LA RECTIFICACIÓN O SUPRESIÓN de aquellos, considerados erróneos o que afectaren ilegítimamente nuestros derechos. Los términos atizados por la Constitución; "INFORMACIÓN" refiera a la acción y efecto de enterar, instruir, y "DATO" a los antecedentes que permiten llegar más fácilmente a conocimiento de una cosa.

La misma resolución estima que el derecho a la protección de datos tiene la naturaleza de un derecho genérico; esto significa que constituye un plexo de derechos específicos, de los cuales se nutre y recibe su contenido. Estos derechos constituyen el derecho a conocer, el derecho a acceder a los datos o información, y el derecho de rectificar o destruir los mismos.

En el caso de Chile, la Corte de Apelaciones de Temuco mediante Resolución No. 61146 señala que:

> en el derecho a la autodeterminación informativa se encuentra implícito en el derecho fundamental a la vida privada [...] el derecho a la autodeterminación informativa consiste en la facultad que tiene una persona de ejercer control sobre sus documentos, información o datos personales que se encuentren en registros o bancos de datos públicos o privados.

Asimismo, en otro fallo la Corte de Apelaciones de Santiago mediante Resolución No. 1849-10 expone que la protección de datos personales contemplada en la Ley 19628:

> Se traduce en el control de las personas sobre sus datos y comprende el derecho a saber sobre la existencia de ficheros o archivos de registro de información de carácter personal,

> públicos o privados, cuáles son sus finalidades y quiénes son los responsables de los mismos, de manera que las personas concernidas puedan conocer los datos propios contenidos en dichos archivos o ficheros, teniendo el derecho a actualizarlos o a solicitar mediante el recurso de hábeas data su rectificación o cancelación.

Se puede considerar que Chile, al igual que Colombia, es uno de los países que más ha avanzado en los últimos años. Así se desprende de la regulación materializada en una Ley específica y en los proyectos constitucionales que buscan reformular su protección mediante un derecho específico.

Finalmente, en Bolivia el Tribunal Constitucional en Sentencia 965/2004 señala:

> El Hábeas Data tiene por objetivo el contrarrestar los peligros que conlleva el desarrollo de la informática en lo referido a la distribución o difusión ilimitada de información sobre los datos de la persona; y tiene por finalidad principal el proteger el derecho a la autodeterminación informática, preservando la información sobre los datos personales ante su utilización incontrolada, indebida e ilegal, impidiendo que terceras personas usen datos falsos, erróneos o reservados que podrían causar graves daños y perjuicios a la persona.

Asimismo, el Tribunal en la Sentencia 496/2015 estima que:

> La acción de protección de privacidad, constituye una garantía constitucional de carácter procesal que puede ser interpuesta ante la jurisdicción constitucional –previo agotamiento de los medios administrativos o judiciales– por cualquier persona natural o jurídica que considere que se vulneran sus derechos a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación por estar impedida de obtener la eliminación o rectificación de sus datos personales registrados en cualquier archivo o banco de datos públicos o privados.

Se puede decir que Bolivia ha pasado de un estado de regulación incierto, previo a la reforma constitucional de 2009, a un sistema más ordenado. Ha llegado a considerar la regulación del tratamiento de datos personales, aunque no con una ley en específica. Sobre todo, se ha consagrado a la protección de datos personales como un derecho de carácter fundamental.

Especial referencia a la situación de Argentina, Uruguay y Perú

El intento de aproximar el sistema latinoamericano al modelo europeo en materia de protección de datos personales de a poco debe cristalizarse.[43] Desde ya han surgido algunas precisiones sobre este proceso de transformación que son necesarias en virtud de la evidente dispersión normativa y diferentes tópicos jurídicos con los que se aborda la regulación del derecho fundamental a la protección de datos personales en Latinoamérica.

Son tres países que a nivel de la CAN merecen una discusión especial en virtud del ordenamiento jurídico que han desarrollado y los reconocimientos que desde el ámbito internacional han recibido.[44]

Argentina y Uruguay han obtenido reconocimiento internacional, y, en los últimos años, Perú ha desarrollado en la Constitución y Leyes Sectoriales niveles adecuados de protección.[45] El marco común de estos países es procurar un régimen jurídico que asigne protección integral de la información personal.[46] Por tanto, a fin de contextua-

---

43. Incluso, como señala Carlos Gregorio en su estudio sobre "Protección de datos personales: Europa *vs.* Estados Unidos, todo un dilema para América Latina" se debería seguir en Latinoamérica la política adoptada por la Unión Europea, es decir: "evitar los inconvenientes de muchas Leyes nacionales de Protección de Datos Personales y lograr una norma común".
44. Como señala Antonio Troncoso, "este reconocimiento lo ha obtenido hasta ahora Argentina en 2003 y [...] Uruguay este año 2012, teniendo en cuenta que su legislación reconoce principios y derechos de protección de datos, establece autoridades de control independientes y los necesarios recursos administrativos y jurisdiccionales". Cfr. Antonio Troncoso, "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel internacional", *Revista Internacional de Protección de Datos Personales*, No. 1 (2012). Conviene precisar que, en el marco europeo el Grupo de Trabajo del artículo 29 de la Directiva 95/46 C/E –en la actualidad derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo que será aplicable a partir del 28 de mayo de 2015– tiene como atribución emitir dictámenes sobre el nivel de protección de datos personales en países terceros que se encuentren fuera de la jurisdicción de la Unión Europea. Es decir, para considerar que un país tercero garantiza un nivel adecuado de protección se evalúa, en particular: a) país de origen; b) orden jurídico general o sectorial vigente; c) normas profesionales y medidas de seguridad vigentes.
45. Aunque Perú no ha sido calificado como país de nivel de protección adecuado, cuenta con el reconocimiento internacional de su autoridad de protección de datos personales dado por la "Conferencia Internacional de Comisionados de Protección de Datos y Privacidad". Sobre este reconocimiento, véase nota 37, en la cual se hace referencia al caso de Colombia. Disponible en ‹http://www.agpd.es/portalwebAGPD/internacional/Conferencias_inter/index-ides-idphp.php›.
46. En breves términos se puede afirmar que la protección integral se deriva del rango constitucional que se asigne a la protección del derecho a la autodeterminación informativa, de las leyes sectoriales y de las políticas públicas y privadas que se implementen en la práctica a través de sus autoridades de control y supervisión.

lizar este estudio y homogeneizar criterios, es importante resaltar la actividad que han desarrollado, ya que, como advierte el mismo Puccinelli, las "diferencias en las regulaciones muchas veces provocan confusiones conceptuales y llevan a amputaciones innecesarias del instituto, que debe ser regulado –constitucionalmente hablando– de una manera simple y abierta, de forma tal que permita la adecuación a las más variadas posibilidades".[47] De esta manera, siguiendo el orden temático propuesto, se realizan las siguientes anotaciones.

Primero, la Constitución Nacional de Argentina en su artículo 43 refiere a la acción amparo para los fines de garantizar la información de carácter personal.[48] Uruguay, según lo dispuesto por los artículos 7, 10, 28, 72 y 332 de la Constitución, materializa su protección en derechos relacionados con la intimidad y el tratamiento de la información. Ante la falta de reconocimiento constitucional así como del hábeas data, tal como señala Puccinelli, las disposiciones antes anotadas "para cierta doctrina encuentra un fundamento similar al amparo y surge de la interpretación lógico-sistemática-teleológica".[49] Asimismo, según el número 6 del artículo 2 de la Constitución, Perú puede considerarse uno de los primeros en señalar el ámbito tecnológico como afectación a los límites de la intimidad; por tanto, se concibe como un "derecho de no suministro de informaciones que afecten la intimidad personal y familiar de manera que el su indebido del poder informático tiene efectos significativos en el seno de las actividades económicas, en relación con la burocracia estatal y la ciudadanía; y hasta en la intimidad personal y familiar".[50]

Segundo, en el ámbito sectorial, en Argentina destaca la Ley 25.326.[51] A más de ser el segundo país latinoamericano con una Ley de Protección de Datos, ha obtenido

---

47. Oscar Puccinelli, "El hábeas data en las provincias argentinas y en la ciudad autónoma de Buenos Aires", *Revista de Derecho PUCP: Revista de Derecho*, No. 1 (1997): 149-76.
48. Como señala Puccinelli "tanto en la Argentina –en los niveles federal y local– como en el derecho latinoamericano, existen variantes de un instituto que en sí no es complicado, pero que muchas veces pareciera no haber sido captado en su esencia por el constituyente, tal vez por su reciente aparición en el mundo jurídico". Puccinelli, "El hábeas data en las provincias argentinas y en la ciudad autónoma de Buenos Aires", 175.
49. Oscar Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de hábeas data a dos décadas de su creación", en *La ciencia del Derecho procesal constitucional: estudios en homenaje a Héctor Fix-Zamudio en sus cincuenta años como investigador del derecho* (México: Instituto de Investigaciones Jurídicas, 2009).
50. Víctor García Toma, *Los derechos fundamentales en el Perú* (Lima: Ed. Jurista, 2008), 187-8.
51. La Ley 25326 de 2000, en su artículo señala que "La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo

reconocimiento a nivel internacional. Son varios los criterios por los cuales la doctrina lo ha justificado plenamente,[52] entre ellos, la previsión de una autoridad administrativa de protección de datos personales como la Dirección Nacional de Protección de Datos Personales (DNPDP).[53] Así también, encontrándose aprobado el Reglamento (UE) 2016/679 de protección de datos personales y por el cual se deroga la Directiva 95/46, en 2015 se ha propuesto ante el Senado de Argentina el Proyecto de Ley sobre "El derecho al Olvido".[54] En este ámbito, Uruguay cuenta con la Ley 18331[55]

---

tercero de la Constitución Nacional". La importancia de una Ley por el estilo ha sido justificada por la doctrina porque "regula a todo aquel que trata datos. Si una persona o entidad recopila datos personales, entonces tiene que cumplir con una serie de obligaciones, desde registrar la base de datos, hasta dar acceso y corrección en caso de que tengan datos erróneos". Pablo Palazzi, "Periodismo de datos y datos personales: algunas reflexiones sobre la aplicación de la ley de protección de datos personales a la prensa en la Argentina", *Revista Latinoamericana de Protección de Datos Personales*, No. 3 (2012).

52. Por ejemplo, se sostiene que: "la ley de Argentina cumple con todos los requerimientos sustantivos que la Unión Europea suele constatar en su examen. De hecho, al analizar la seguridad del país, el Grupo del artículo 29 sobre Protección de Datos constató un satisfactorio nivel de protección en las disposiciones sustantivas, tales como aquellas relativas al ámbito de aplicación, los principios generales aplicables al tratamiento de datos, los derechos del titular de datos personales, y las obligaciones de las entidades responsables de dicho tratamiento". Cfr. Alberto Cerda Silva, "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, No. 1 (2011): 327-56.
53. La DNPDP cumple un papel importante en su objetivo de precautelar la protección de este derecho fundamental; por ello, en noviembre de 2016 ha sido nombrada como miembro del Comité Ejecutivo de la RIPD junto con las autoridades de protección de Colombia y México.
54. El afán de mantener un orden jurídico de protección de datos personales acorde a escenarios internacionales ha precisado la formulación de este tipo de normas que se consideran como una de las novedades dentro del Reglamento (UE) 2016/679. Al caso Pablo Palazzi señala que "En cuanto a Argentina, no hay normas en la Ley 25326 como las que existen en la directiva (art. 4). Por eso, la determinación de la ley aplicable al tratamiento de datos personales en internet es difícil de abordar y debe recurrirse a los principios generales del Derecho, o desarrollar nuevos criterios para poder determinar la competencia territorial de las normas locales en internet [...] En Argentina los tribunales también reconocieron el derecho al olvido en materia de informes comerciales antes de que la Ley 25326 los contemplara en forma expresa. Por ende no parece difícil que el derecho al olvido tenga andamiento jurisprudencial antes de que la Ley 25326 lo recepte en una futura reforma legislativa, aunque se deberá tener en cuenta las limitaciones que la Ley 25326 establece para la prensa y cómo impactan en los buscadores". Véase Pablo Palazzi, *El reconocimiento en Europa del derecho al olvido en Internet* (Buenos Aires: La Ley, 2014). Disponible en ‹http://www.privacylatam.com/wp-content/uploads/2014/06/Diario-9-6-14.pdf›.
55. En 2008 se promulga la Ley 18331 con la finalidad de reconocer como un derecho fundamental e inherente a la persona humana a la protección de datos personales. El artículo 3 de esta Ley enmarca su objeto señalando que: "El régimen de la presente ley será de aplicación a los datos personales

destinada a proteger los datos personales y establecer su garantía mediante el hábeas data.[56] Esta Ley dispuso la creación de la Unidad Reguladora y de Control de Datos Personales (URCDP) que se ha enmarcado como autoridad de supervisión y control de este derecho fundamental.[57] En este mismo sentido, en Perú la Ley 29733[58] prevé la protección del derecho fundamental contemplado en el número 6 del artículo 2 de la Constitución.[59] Complementariamente, esta ley dispone que el Ministerio de Justicia (hoy, Ministerio de Justicia y Derechos Humanos) a través de la Dirección General de Protección de Datos Personales (DGPDP)[60] se promueve como autoridad de control.

Por último, en referencia a las definiciones jurisprudenciales, la Corte Suprema de Justicia de Argentina mediante sentencia XXXlll señala que:

> La protección legal se dirige a que el particular interesado tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga. En tal sentido, este derecho forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los

---

registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado".

56. El artículo 37 de la Ley No. 18331 refiere: "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".
57. A partir de la Ley No. 18331, la URCDP se configura como un órgano con amplia autonomía técnica y jurídica que dicta resoluciones, dictámenes y elabora informes para la observancia del derecho fundamental a la protección de datos personales. Su desarrollo ha sido importante a tal punto que, en noviembre de 2016, fue designada para ejercer la Presidencia de la RIPD.
58. La Ley 29733 de 2011 pretende regular el tratamiento de datos personales y desarrollar propiamente el contenido del derecho a la autodeterminación informativa consagrado en la Constitución. El artículo 1 de esta Ley prescribe en su objeto que "La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen".
59. Tal como señala Zamudio, mediante esta Ley "se 'coloca' legalmente el epígrafe al citado numeral constitucional, definido en algunas oportunidades por la jurisprudencia del Tribunal Constitucional como el derecho a la autodeterminación informativa". María de Lourdes Zamudio, "El marco latinoamericano y Ley de Protección de Datos Personales en Perú", *Revista Internacional de Protección de Datos Personales* (2012).
60. Tal como señala el inciso 3 del artículo 32 de la Ley 29733: "Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la presente Ley y de su reglamento. Para tal efecto, goza de potestad sancionadora, de conformidad con la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley 26979, Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces".

> bienes que integran la personalidad. El señorío del hombre sobre sí se extiende a los datos sobre sus hábitos y costumbres, su sistema de valores y de creencias, su patrimonio, sus relaciones familiares, económicas y sociales, respecto de todo lo cual tiene derecho a la autodeterminación informativa.

La misma resolución, sobre el hábeas data agrega que:

> A esta decisión se le atribuye la configuración del concepto de "autodeterminación informativa" o libertad informática, que es reconocido actualmente en forma predominante como el fundamento del hábeas data en las legislaciones que contemplan derechos análogos [...] Según este concepto es el ciudadano quien debe decidir sobre la cesión y uso de sus datos personales. Este derecho –se dijo– puede ser restringido por medio de una ley por razones de utilidad social, pero respetando el principio de proporcionalidad y garantizando que no se produzca la vulneración del derecho a la personalidad.

En este mismo sentido, en Uruguay la sentencia No. 12 de 2008 del Tribunal de Apelaciones refiere, en cuanto al hábeas data, que "el procedimiento previsto por los arts. 37 a 45 de la Ley No. 18331 de 11/8/2008 es el común que el ordenamiento jurídico prevé para las pretensiones que tengan por objeto exclusivo el hábeas data, o sea, el acceso a la información en bases de datos, su rectificación, inclusión o supresión". Este mismo Tribunal, en relación al derecho fundamental a la protección de datos personales, en la sentencia No. 4 de 2015 señala que:

> Hubiera sido preferible que la actora citara también, expresamente y no de modo tangencial o implícito en su exposición, el derecho a la seguridad en la protección de datos personales, a la intimidad, inviolabilidad de las comunicaciones y exclusión de las acciones privadas del quehacer estatal cuando no afectan el ordenamiento jurídico, garantizados por los artículos 7 y 10 de la Constitución para todo habitante de la República y esenciales en un Estado de Derecho sometido al régimen democrático-republicano de gobierno.

Por su parte, el Tribunal Constitucional de Perú en la Sentencia No. 71797-2002 apunta que:

> El derecho a la autodeterminación informativa está destinado a proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2 de la Constitución.

La misma sentencia, sobre el hábeas data, agrega que:

> Comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona... Asimismo, con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados.

En este contexto, siguiendo el ejemplo marcado por el reconocimiento internacional de Argentina y Uruguay, Perú se constituye campo el país de la CAN que últimamente ha mejorado su marco de regulación y garantía del derecho fundamental a la protección de datos personales. Le sigue Chile en este proceso que, hasta marzo de 2017, ha promovido la reforma del Ley 19628 por la cual se prevé la actualización y modernización del marco normativo e institucional para la defensa del derecho a la protección de datos personales. En este último caso se destaca la implementación de una Agencia de Protección de Datos Personales.

Estado de la situación en Ecuador

Antecedentes

En Ecuador, la incorporación del derecho fundamental a la protección de datos personales tiene su origen en la reforma gestada por la Asamblea Constituyente de plenos poderes[61] elegida para debatir y aprobar el contenido de la Constitución de 2008. A propósito del socialismo del siglo XXl, se ha idealizado el denominado "neoconstitucionalismo andino" que representa un proyecto constitucional histórico[62] en

---

61. El Poder Constituyente de la Asamblea afirmó que esta asume y ejerce "plenos poderes" según el Mandato Constituyente 1, es decir: "Las decisiones de la Asamblea Constituyente son jerárquicamente superiores a cualquier otra norma del orden jurídico y de obligatorio cumplimiento para todas las personas naturales, jurídicas y demás poderes públicos sin excepción alguna. Ninguna decisión de la Asamblea Constituyente será susceptible de control o impugnación por parte de alguno de los poderes constituidos".
62. Según Ávila Santamaría, el proyecto político de la Revolución Ciudadana, materializado en la Constitución de Montecristi en 2008, "tiene instituciones que no solamente abren la puerta a la imaginación de posibilidades de un mundo distinto, sino que constituyen una oportunidad para la transformación de la realidad" en donde más personas son ciudadanas, es decir, mediante el reconocimiento de más libertades fundamentales la ciudadanía es más extensa. Cfr. Ramiro Ávila Santamaría, *El neoconstitucionalismo andino* (Quito: Universidad Andina Simón Bolívar, 2016), 71-75.

la garantía de los derechos fundamentales, afianzado en la interpretación del ejercicio y la exigibilidad de los derechos más esenciales del ser humano.

Con este antecedente, la Asamblea Constituyente registra a través de acta 050[63] el debate legislativo sobre el derecho a la protección de datos personales. De los informes[64] presentados por la Mesa Constituyente No. 1, se expone la Carta de Derechos aprobada por la Mesa[65] en donde entre otros aspectos para su fundamentación se hizo referencia a estándares internacionales establecidos en diversos tratados de derechos humanos ratificados por Ecuador y que constituyeron la base para los contenidos mínimos de estos derechos. La propuesta de la Carta de Derechos Civiles[66] consideró

---

63. En los antecedentes del acta 50 de la Asamblea Nacional Constituyente, en relación a la propuesta de la Carta de Derechos, se considera que esta surge a partir de un proceso amplio de reflexión colectiva con la ciudadanía: a) propuestas y sugerencias de más de 160 representantes de varios sectores de la población; b) 120 propuestas mediante internet; y, c) 6 mesas itinerantes, con el objeto de recopilar propuestas y promover la participación ciudadana. De esta manera, el 15 de mayo de 2008, la Mesa Constituyente No. 1 de Derechos Fundamentales y Garantías Constitucionales conformada por trece legisladores –ocho del bloque de gobierno (Alianza País) y 5 de oposición escogidos de entre varios partidos políticos– pone en conocimiento del Pleno de la Asamblea para primer debate los textos constitucionales referentes a los derechos civiles en donde se incluye el derecho a la protección de datos personales.
64. Para el inicio de este primer debate sobre la Carta de Derechos Civiles –con ochenta y dos asambleístas presentes en el seno legislativo–, se asume que, según el informe del asambleísta Jaime Abril, la propuesta fue aprobada por consenso en la Mesa con Informe de Mayoría con excepción del asambleísta Rafael Estévez, quien expone su Informe de Minoría pero que en nada debate la aprobación del derecho a la protección de datos de carácter personal.
65. Desde esta perspectiva –a diferencia de la Constitución de 1998 que incluía los derechos civiles como números de un único artículo–, la Mesa consideró necesario que cada uno de los derechos a los que se hace referencia en la Carta de Derechos Civiles deberán ser enunciados como artículos independientes para proporcionarles mayor énfasis y reconocimiento. Así surge por primera vez la propuesta del derecho fundamental a la protección de datos de carácter personal que dentro del articulado correspondiente a los derechos civiles se presentó de la siguiente manera: "Artículo innumerado, Derecho a la protección de datos de carácter personal: a) El Estado garantiza el derecho a decidir sobre los datos personales; b) La Ley regulará la recolección, archivo, procesamiento, distribución o difusión de la información de estos datos. Para todo esto se requerirá la autorización del titular o la prescripción de la ley".
66. Se considera en esta exposición que –a propósito de los sesenta años del nacimiento de la Declaración Universal de los Derechos Humanos, a la fecha en que la Asamblea Constituyente inicia el proceso de reforma constitucional–, en última instancia, estos derechos existen para proteger y asegurar el ejercicio y respeto de los derechos fundamentales en sus ciudadanos. Se puede tomar como referencia la alusión de que para la reforma constitucional de la Carta de Derechos Civiles propuesta por la Mesa Constituyente se amplía a treinta y cuatro derechos a diferencia de la Constitución de 1998 con veinte y seis derechos. Es importante destacar que la mayoría de los artículos propuestos fueron aprobados por unanimidad; asimismo, al hacer referencia a un régimen de derechos fundamentales de carácter innovador y progresista, uno de estos precedentes puede estar invocado precisamente

que, entre otros derechos, el nuevo derecho a la autodeterminación informativa define la acción del Estado en función de la cual se deben organizar las estructuras del poder del Estado bajo un régimen innovador, revolucionario y progresista.

Ahora bien, la Asamblea Constituyente registra a través de acta 067[67] la votación en pleno del texto definitivo sobre este derecho fundamental. A pesar de que no existe una referencia específica en actas legislativas sobre el origen de la propuesta, se puede colegir que la inserción de este nuevo derecho supondría ser el resultado del proceso de reflexión colectiva con la ciudadanía. También se puede afirmar que su derivación respondería a los estándares internacionales establecidos en los Tratados y Convenios de Derechos Humanos. Por tanto, su base se centraría en dos de los principios que integran el denominado "neoconstitucionalismo andino" enmarcado principalmente en la constitucionalización de nuevos y más derechos fundamentales para los ciudadanos, viabilizados mediante la denominada democracia comunitaria o participativa.[68]

---

hacia la determinación del derecho a la protección de datos de carácter personal como un derecho fundamental ya que en relación a la Constitución de 1998 no se encontraba reconocido como tal.

67. El 24 de junio de 2008, la Mesa Constituyente No. 1 de Derechos Fundamentales y Garantías Constitucionales pone en conocimiento del Pleno de la Asamblea, para su aprobación, los textos constitucionales referentes a los derechos civiles en donde se incluye el derecho a la protección de datos personales. El texto final se presentaba de la siguiente manera: "Toda persona tiene derecho a acceder y decidir sobre información y datos de carácter personal y a que estos sean protegidos. b) Para la recolección, archivo, procesamiento, distribución o difusión de esos datos o información se requerirá la autorización del titular o la prescripción de la Ley". En este orden de ideas, se menciona que los cambios principales realizados al texto definitivo son por ejemplo sobre el derecho a la reserva que garantizará que no se pueda utilizar información relativa al pensamiento político y no solo a la filiación política; y, la reformulación del derecho a la protección de datos de carácter personal, estableciéndose el derecho a acceder y decidir sobre información y datos de carácter personal y a que estos sean protegidos, además que para la recolección, archivo, procesamiento, distribución o difusión de esos datos se requerirá la autorización del titular o la prescripción de la ley cuando sea pertinente. La votación sobre el artículo 1 de los derechos civiles se produce con la presencia de noventa y cuatro asambleístas presentándose: setenta y tres votos afirmativos; cinco votos negativos; cero blancos y dieciséis abstenciones.
68. Como apunta Ávila Santamaría, la democracia participativa podría entenderse como una forma de manifestación de opinión permanente de los ciudadanos, es decir "donde todas las personas y nacionalidades tienen la genuina posibilidad de opinar" y que, en todo caso surge como complemento de otras formas de democracia. Cfr. Ávila Santamaría, *El neoconstitucionalismo andino*, 30 y 84.

Contextualización en la Carta Magna, Régimen Sectorial y Jurisprudencia

La protección de datos personales evolucionó desde la protección constitucional del hábeas data y derechos a la intimidad personal y familiar en la Constitución de 1998 hasta su reconocimiento como un derecho fundamental en 2008 situándose como un "derecho de libertad".[69] Sobre el tema, la doctrina considera que "la Constitución de la República reconoce el derecho, libertad o autodeterminación informática o informativa [...] Esta amenaza se ha agravado, ahora como nunca, con el avance de la ciencia y la tecnología".[70]

A la luz del derecho a la autodeterminación informativa es relevante que se haya completado y perfeccionado la acción jurisdiccional del hábeas data[71] con el objeto de buscar una protección más efectiva frente al tratamiento de la información. Sin embargo, a falta de una ley general, también se ha intentado ampliar su contenido en leyes sectoriales en donde destacan la Ley de Comercio Electrónico, Ley del Sistema Nacional de Registro de Datos Públicos, Ley Orgánica de Comunicación y Ley Orgánica de Telecomunicaciones.[72]

---

69. Precisamente, uno de los cambios significativos de la actual Constitución es que se "elimina la clásica división de derechos civiles, políticos, y económicos, sociales y culturales. En su lugar utiliza una división puramente temática (derechos de participación, derechos de libertad, etc.)". Cfr. Agustín Grijalva Jiménez, *Constitucionalismo en Ecuador* (Quito: Corte Constitucional para el Período de Transición, 2012), 28. Así, el número 19 del artículo 66 de la Constitución reconoce como un derecho de libertad: "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".
70. Julio César Trujillo, "Las garantías jurisdiccionales", *Vlex* (base de datos). Disponible en ‹https://app.vlex.com/#WW/vid/515951146/graphical_version›.
71. Se debe anotar que la Constitución asegura la protección de este derecho fundamental mediante la acción de hábeas data contemplada en el artículo 92. Esta garantía reconoce facultades al titular de la información personal sobre "decidir a quién, para qué y cuándo hace conocer sus datos y, en consecuencia, autoriza archivarlos, procesarlos y difundirlos y, a continuación, le reconoce otros derechos tendientes a controlar el trato y destino que ha dado a esos datos el responsable del banco en el que autorizó sean registrados". Cfr. Trujillo, "Las garantías jurisdiccionales".
72. En cuanto al desarrollo de normativas específicas o sectoriales, "en varios países de la región se han intentado proyectos legislativos que regulan esta actividad [...] Luego de los debates parlamentarios se incluyeron algunas normas en las Leyes de Datos Personales y hábeas data, las que resultan insuficientes para regular la actividad a la luz de los conflictos observados en la jurisprudencia". Cfr. Carlos Gregorio, "Protección de Datos Personales: Europa *vs.* Estados Unidos, todo un dilema para América Latina". En el caso de Ecuador, se debe agregar que actualmente se ha presentado en la Asamblea Nacional el "Proyecto de Ley Orgánica de la Protección de los Derechos a la Intimidad y

En la materia, la Corte Constitucional ha sentado el primer precedente que se encuentra recogido en la Sentencia No. 1-14-PJP-CC de 2014. En concreto, la Corte señala:

> La autodeterminación informativa está supeditada, entonces, a la existencia de información que atañe a determinado sujeto y a la necesidad de que este tenga una esfera mínima de actuación libre respecto de dicha información, sobre la cual no debería existir una interferencia ilegítima por parte de terceros; asimismo, implica la posibilidad de que dentro de los límites que franquean la Constitución y la Ley, se tenga capacidad para ejercer cierto control sobre el uso que se haga de tal información, aunque el poseedor de la misma sea otra persona (...) En el caso de la autodeterminación informativa, como parte del derecho a la protección de datos personales, implica la necesidad de garantizar la protección de la esfera íntima de las personas, así como la posibilidad de ejercer control sobre los datos personales del sujeto, aunque no se encuentren en su poder.

Esta misma resolución, sobre el hábeas data aclara que:

> Como mecanismo de garantía del derecho a la protección de datos personales, no podrá ser incoado como medio para requerir la entrega física del soporte material o electrónico de los documentos en los que se alegue está contenida la información personal del titular sino para conocer su existencia, tener acceso a él y ejercer los actos previstos en el artículo 92 de la Constitución de la República.

Al respecto, más allá del cambio de denominación o temática –en relación a los derechos contemplados en la Constitución de 1998–, uno de los méritos más altos está el haberse atribuido autonomía al derecho fundamental que se desprende del tratamiento de la información personal. Le sigue, en importancia, la ampliación y el desarrollo de la garantía constitucional del hábeas data al habérsele incorporado más facultades procesales y garantistas sobre este derecho fundamental. Sin embargo, es notorio que en la práctica se requiere mucho más. Tal como lo señala el CJI en su 86 período ordinario de sesiones: "las respuestas a estos adelantos y amenazas han sido diferentes en distintas regiones del mundo. En las Américas no parece haber surgido un enfoque 'regional' uniforme y coherente".[73]

Privacidad sobre los Datos Personales" que, revisado de modo preliminar, carece de fundamentos a partir de modelos jurídicos comparados que aquí se han señalado y que, en todo caso, merece otro análisis pormenorizado.

73. A esta opinión del CJI, como señala Julio César Trujillo, se precisa que el legislador ecuatoriano mantiene una deuda pendiente en la necesidad de mantener salvo la información de carácter personal frente a su tratamiento automatizado. En tal virtud, en Ecuador el ordenamiento jurídico disperso conjuntamente con las recomendaciones elaboradas por la OEA significaría la base para una pro-

En el caso de Ecuador, a pesar de que la idea que se propondrá resulta de un modelo de integración, bien puede señalarse que las bases para un ordenamiento jurídico que contribuya a este fin se encuentran fijadas –a propósito del proyecto de Ley Orgánica sobre datos personales–, primero, en la articulación de una ley general afianzada en los principios y estudios elaborados por la OEA para consolidación de una Ley Interamericana, y, segundo, en la materialización de mecanismos para la defensa y tutela del derecho a la autodeterminación informativa a través de una autoridad de control. Más aún, tras haberse firmado un acuerdo comercial con la Unión Europea a finales de 2016, Ecuador se encuentra en momento decisivo en virtud de contar con un marco jurídico homogéneo por cuanto –de este tipo de relaciones comerciales sobre integración económica– se desprende la necesidad de regular temas vinculados al flujo transfronterizo de datos personales.[74]

En este sentido, dentro de una era globalizada, la protección de los derechos fundamentales es de gran importancia debido a que en el contexto jurídico debe converger su desarrollo integral con el aseguramiento del ejercicio pleno de sus derechos fundamentales acorde a la evolución del paradigma tecnológico y constitucional. Por tanto, se plantea la obligación de equilibrar y regular el tratamiento de la información personal –en el ámbito público y privado– garantizando al titular de la información la capacidad de ejercer control sobre el uso y finalidad que se haga respecto de dicha información.

Hacia un modelo Interamericano de Integración para la protección del derecho fundamental a la autodeterminación informativa

Como ha señalado el CJI, al parecer no existe uniformidad normativa en las Américas para asignar protección semejante del derecho fundamental a la autodeterminación informativa en este ámbito regional. A contra sensu, en el caso europeo una de las

---

puesta uniforme y coherente de una ley general para la protección de los datos de carácter personal. Cfr. Trujillo, "Las garantías jurisdiccionales".

74. Según expone Antonio Troncoso, la integración económica europea dependía en gran medida de contar con un modelo homogéneo que garantice la protección de datos personales. Como bien señala: "El movimiento de personas, de mercancías y de capitales implica también el intercambio de información personal lo que obliga a tener unos estándares comunes de protección de datos personales que permitan este intercambio de información. Y ya fuera del ámbito de la Unión Europea, el derecho fundamental a la protección de datos personales es un derecho esencial para el mantenimiento de relaciones personales y comerciales con otros países que conllevan la existencia de flujos de información personal". Cfr. Troncoso, *La protección de datos personales: en busca del equilibrio*, 170.

virtudes ha sido universalizar principios y criterios jurídicos de protección a través de Directivas y Reglamentos orientados a establecer en cada país un marco homogéneo de regulación.

En la práctica, en términos garantistas, es evidente que el derecho a la autodeterminación informativa requiere de las condiciones necesarias para su pleno reconocimiento y ejercicio en virtud de la pluralidad de bienes jurídicos que integran su protección. Por ello, la protección de datos personales "en las sociedades actuales precisan de un equilibrio entre el flujo de informaciones... con la garantía de la privacidad de las personas".[75]

Autores como Antonio Troncoso y Pérez Luño coinciden en la necesidad de "buscar equilibrio" entre la administración y los ciudadanos. Este planteamiento sugiere en gran medida un "pacto social" que garantice la proporcionalidad de las libertades que se desprenden del derecho a la protección de datos personales. Para este fin, es necesario "un adecuado ordenamiento jurídico de la informática, capaz de armonizar las exigencias de información propias de un Estado avanzado con las garantías de los ciudadanos".[76] Por tanto, nos encontramos "ante la necesidad de proteger al hombre frente a las tecnologías de la información y las comunicaciones; ante la obligación de hacer presentes los derechos y tutelarnos en la era de internet".[77]

En este sentido, el modelo de regulación europea sustentado en la integración comunitaria significa para el sistema interamericano –y por ende en la CAN– un referente para la universalización de principios y preceptos legales para la garantía del derecho fundamental a la protección de datos personales. Precisamente, son dos antecedentes que permiten encaminar esta propuesta. El primero, vinculado a los "Doce principios para la Privacidad y la Protección de Datos Personales" adoptados por la OEA; y el segundo, relacionado a la adecuación normativa, conforme a estándares internacionales, incorporada por Argentina, Uruguay, Perú, Colombia y, Chile últimamente. En ambos casos, como se ha reiterado, estos antecedentes se marcan por la influencia europea.

De esta manera, las bases para un modelo Interamericano de Integración[78] –que asegure la protección del derecho fundamental a la autodeterminación informativa– se pueden enunciar en dos presupuestos y a la vez necesidades, a saber:

---

75. Antonio Pérez Luño, *Derechos humanos, Estado de derecho y Constitución* (Madrid: Tecnos, 2010), 363.
76. Ibíd., 363.
77. Troncoso, *La protección de datos personales: en busca del equilibrio*, 33.
78. Tal como señala Antonio Troncoso: "una legislación estrictamente nacional de protección de datos personales no es efectiva ya que los tratamientos de datos personales se desarrollan por internet a

a) Un Reglamento Interamericano que impida dispersión normativa entre los países miembros y que sea compatible con instrumentos internacionales para la protección de datos personales.
b) Adoptar medidas legislativas que, tendientes a unificar las legislaciones internas y políticas sectoriales de los países miembros, aseguren la materialización del derecho a la autodeterminación informativa y su defensa mediante la creación de autoridades de control.

CONCLUSIONES

a) En los ordenamientos jurídicos de la CAN, al igual que en la Unión Europea, la base para el desarrollo del derecho a la autodeterminación informativa ha sido la transición desde la protección del derecho a la intimidad hacia el reconocimiento constitucional de un derecho autónomo vinculado a la acción jurisdiccional del hábeas data. De ahí que su regulación, a partir de la tutela constitucional, ha requerido la implementación de leyes generales que desarrollen en la práctica mecanismos de protección sobre los bienes jurídicos que se desprenden de este nuevo derecho fundamental.
b) Existen notables diferencias entre los países que han recibido reconocimiento internacional en relación con otros que todavía empiezan o se encuentran en proceso de consolidar un modelo adecuado en el régimen sectorial. Por consiguiente –sobre la base de los Principios y estudios realizados por la OEA, y la experiencia incorporada por Argentina, Uruguay y Perú–, la necesidad de crear un marco interamericano para la regulación de los datos personales es estrictamente necesaria en virtud de proteger integralmente el tratamiento de la información personal en el marco de una sociedad globalizada por la economía y las tecnologías de la información y comunicación.
c) Consagrar un modelo interamericano de integración para la protección de este derecho fundamental no es una idea extraña. En la materia, la experiencia de la Unión Europea ha tenido resultados favorables a partir de un marco regulador común con base al Convenio 108, Directiva 95/46/UE y Reglamento 2016/679/UE destinados a materializar –en el régimen jurídico interno e internacional de

---

través de redes internacionales [...] lo que exige que, al menos, la normativa de protección de datos personales –y en el futuro las propias instituciones de tutela– tengan un carácter supranacional. Cfr. Troncoso, *La protección de datos personales: en busca del equilibrio*, 170.

sus Estados Miembros– un nivel adecuado de protección del derecho fundamental de datos personales dentro del mundo de las tecnologías.

d) La propuesta de la OEA debe desembocar en la implementación de una Ley o Reglamento Interamericano que permita desarrollar en el ámbito regional y régimen jurídico interno de sus Estados Miembros un marco equilibrado y homogéneo que asegurare, en la práctica, su protección integral. Con esta condición, se exige la incorporación de autoridades de control y supervisión que –incluso a nivel supranacional– estén facultadas para ejercer con autonomía e independencia la tutela y garantía del derecho fundamental a la autodeterminación informativa.

e) En Ecuador el reconocimiento constitucional a la protección de datos personales como un derecho fundamental ha sido el resultado de la constitucionalización de nuevos derechos viabilizados a través de la denominada democracia participativa. La jurisprudencia ha ratificado la necesidad de ejercer control sobre la información personal por lo que se hace evidente la necesidad de contar con una Ley General de Protección de Datos Personales que –como medio de integración económica y jurídica– posibilite la protección sistemática de los datos personales dentro de un mismo marco común en una sociedad globalizada. Para este último fin, la articulación de una Ley por el estilo debe estar afianzada en los principios desarrollados por la OEA y luego, en la práctica, tutelada con suficientes mecanismos de garantía que precisan la idea de contar con una autoridad de control y supervisión como el caso de Argentina, Uruguay, Perú y Colombia.

BIBLIOGRAFÍA

Ávila Santamaría, Ramiro. *El neoconstitucionalismo andino*. Quito: Universidad Andina Simón Bolívar, 2016.

Cerda Silva, Alberto. "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea". *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso* (2011).

Chivi, Idón. *Nueva Constitución Política del Estado: conceptos fundamentales para su desarrollo normativo, glosario de la Nueva Constitución Política del Estado*. La Paz: Vicepresidencia del Estado Plurinacional, 2010.

Doneda, Danilo. "A proteção dos dados pessoais como direito fundamental no direito brasileiro". *Revista Latinoamericana de Protección de Datos Personales* (2012).

---. "O habeas data no ordenamento brasileiro e a proteção de dados pessoais: uma integração ausente". *Revista de Derecho Comunicaciones y Nuevas Tecnologías* (2007).

García Toma, Víctor. *Los derechos fundamentales en el Perú*. Lima: Ed. Jurista, 2008.

Gregorio, Carlos. "Protección de datos personales: Europa *vs.* Estados Unidos, todo un dilema para América Latina". En Raúl Márquez Romero, coord., *Transparentar al Estado: la experiencia mexicana de acceso a la información*. México: Instituto de Investigaciones Jurídicas, 2005.

Grijalva Jiménez, Agustín. *Constitucionalismo en Ecuador*. Quito: Corte Constitucional para el Período de Transición, 2012.

Hassmer, Winfried, y Alfredo Chirino Sánchez. *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales*. Buenos Aires: Editores del Puerto, 1997.

Jijena, Renato. "Tratamiento de datos personales en el Estado y acceso a la información pública". *Revista Chilena de Derecho y Tecnología* (2013).

Linden, Regina, y Temis Limberger. "Banco de datos de informaciones genéticas y la administración pública como concretizadora de la protección de datos personales y de la dignidad humana". En José Luis Barzallo, coord., *Memorias XVI Congreso Iberoamericano de Derecho e Informática*. Quito: Ministerio de Justicia, Derechos Humanos y Cultos, 2012.

Losing, Norbert. "La justicia constitucional en Paraguay y Uruguay". *Anuario de Derecho Constitucional Latinoamericano* (2002).

Murillo de la Cueva, Pablo, y José Luis Piñar. *El derecho a la autodeterminación informativa*. Madrid: Fontamara, 2011.

Núñez, Víctor Manuel. *Protección de datos personales*. Asunción: Centro Internacional de Estudios Judiciales, 2010.

Palazzi, Pablo. "Avances en la protección de datos personales en América Latina". *Revista Latinoamericana de Protección de Datos Personales* (2011).

---. *El reconocimiento en Europa del derecho al olvido en internet*. Buenos Aires: La Ley, 2014.

---. "Periodismo de datos y datos personales: algunas reflexiones sobre la aplicación de la ley de protección de datos personales a la prensa en la Argentina". *Revista Latinoamericana de Protección de Datos Personales* (2012).

Pérez Luño, Antonio. *Derechos humanos, Estado de derecho y Constitución*. Madrid: Tecnos, 2010.

Puccinelli, Oscar. "Apuntes sobre el derecho, la acción y el proceso de hábeas data a dos décadas de su creación". En *La ciencia del Derecho procesal constitucional: estudios en homenaje a Héctor Fix-Zamudio en sus cincuenta años como investigador del derecho*. México: Instituto de Investigaciones Jurídicas, 2009.

---. "El hábeas data en las provincias argentinas y en la ciudad autónoma de Buenos Aires". *Derecho PUCP: Revista de la Facultad de Derecho*, No. 1 (1997).

Tovar, Luis Freddyur. "Positivación y protección de los derechos humanos: aproximación colombiana". *Revista Criterio Jurídico* (2008).

Troncoso, Antonio. "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel internacional". *Revista Internacional de Protección de Datos Personales* (2012).

---. *La protección de datos personales: en busca del equilibrio*. Valencia: Tirant lo Blanch, 2010.

Trujillo, Julio César. "Las garantías jurisdiccionales". *Vlex* (base de datos). Disponible en ‹https://app.vlex.com/#WW/vid/515951146/graphical_version›.

Zamudio, María de Lourdes. "El marco latinoamericano y Ley de Protección de Datos Personales en Perú". *Revista Internacional de Protección de Datos Personales* (2012).

Fecha de recepción: 14 de marzo de 2017
Fecha de aprobación: 15 de mayo de 2017

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

El Reglamento Europeo (UE) 2016/679: análisis de un claroscuro

*Marcel Moritz** y *Valentin Gibello***

RESUMEN

La Directiva 95/46/CE del 24 de octubre de 1995 fue el primer instrumento jurídico para la regulación de la protección de datos en la Unión Europea. Esta Directiva será sustituida por el Reglamento (UE) 2016/679, a partir del 28 de mayo de 2018.

Este artículo aborda de manera crítica el nuevo Reglamento Europeo, se presentan sus objetivos, y se destaca la importancia de crear un Reglamento en lugar de una nueva Directiva sobre protección de datos personales. Además, se describe el fortalecimiento de la protección de datos personales en la Unión Europea, al tenor de los desafíos tecnológicos de la actualidad. Sin embargo, varios analistas consideran que el nuevo Reglamento genera dudas por cuanto pretende beneficiar a los responsables del tratamiento de datos a través de la aplicación de una metodología de análisis de riesgos. Este doble enfoque genera muchas incertidumbres jurídicas que se discuten a lo largo del texto.

Palabras clave: datos personales, protección de datos, privacidad, derechos fundamentales, derecho al olvido, Unión Europea, análisis de gestión de riesgos.

ABSTRACT

The Directive 95/46/CE from October 24th 1995 was the first legal instrument for the regulation of data protection in the European Union. This directive will be replaced by the Regulation (UE) 2016/679, from May 28th 2018.

This paper abords in critical way this new European Regulation, presents its purposes, and the importance of creating a Regulation instead of a new data protection directive. Furthermore, this paper describes the strenghtening of european data protection law in relation to the challenges of today's technology.

Nevertheless, some analysts consider that the new Regulation generates many doubts because it aims to benefit data controllers by establishing a risk based

* Director del Máster en Derecho Digital, Université Lille 2 Droite et Santé, CERAPS.

** Candidato a doctor, Université Lille 2 Droite et Santé, CERAPS.

approach. This double perspective creates many ambiguities that are discussed along the contents of this paper.

KEYWORDS: personal data, data protection, privacy, fundamental rights, right to be forgotten, european union, risk based approach.

FORO

INTRODUCCIÓN

Conscientes de la transición hacia una economía centralizada en los datos, la Comisión Europea anunció la creación del mercado único digital (digital single market)[1] en mayo de 2015. La Comisión presidida por *Jean-Claude Junker* tuvo la prioridad de agregar a la economía digital dentro de los objetivos de la Unión, a través de la creación de un mercado interno de libre competencia de acuerdo con los valores de la Unión, y en particular, con la protección de los derechos humanos.

En esta perspectiva, y paralelamente al establecimiento de medidas de regulación de esta economía (enmarcado de las tarifas de itinerancia, umbral común del IVA, etc.), la Comisión ha acelerado el proceso de adopción de una importante reforma de la Directiva 95/46/CE del 24 de octubre de 1995, la cual se basa en las leyes nacionales de los estados miembros. La reforma que fue propuesta en 2012 es crucial para los actores de este mercado único digital, y ha sido objeto de intensas negociaciones durante todo el proceso legislativo, hasta su publicación en el Diario Oficial de la Unión Europea el 4 de mayo de 2016.[2]

Plasmado en un Reglamento, este tiene la intención de poner fin a las disparidades que aparecieron como resultado de la transposición de la Directiva a las leyes nacionales de los veintiocho (28) estados miembros, e instaurar en todos ellos el mismo alto nivel de protección de los datos personales y derecho a la vida privada.[3]

---

1. La página oficial de esta prioridad de la Unión, disponible en ‹https://ec.europa.eu/priorities/digital-single-market_en›. Consulta: 15 de enero de 2017.
2. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 relativo a la protección de personas físicas con respecto al tratamiento de datos de carácter personal y la libre circulación de estos datos. Disponible en ‹http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC›.
3. Cuya protección está garantizada por el artículo 8 de la Convención Europea de Derechos Humanos

Este ambicioso texto reafirma los principios preexistentes en una nueva forma jurídica, aportando innovaciones significativas, pero a la vez dando nacimiento a algunas ambigüedades.

UN REGLAMENTO CON OBJETIVOS AMBICIOSOS[4]

En un primer momento, el objetivo del Reglamento aparece más en la forma que en la materialidad de sus disposiciones (a). Sin embargo, un análisis más detallado permite descubrir cambios que pueden engendrar consecuencias significativas (b).

Una evolución ampliamente formal de la legislación europea

La contribución más importante de la solución radica probablemente en su naturaleza jurídica. En efecto, al contrario de una Directiva Europea que no obligaba al cumplimiento de sus objetivos por parte de los estados miembros, por suponer únicamente la transposición de sus textos en el derecho interno, el Reglamento pretende ser una ley uniforme. De acuerdo con el artículo 288 del Tratado de funcionamiento de la Unión Europea, un Reglamento "será obligatorio en todos sus elementos y [...] es directamente aplicable en todos los Estados miembros". Por lo tanto, la regulación "produce efectos inmediatos y es, como tal, capaz de crear derechos individuales que los órganos jurisdiccionales nacionales tienen la obligación de proteger".[5]

Este es un punto de gran importancia, dado que una de las debilidades del derecho europeo de protección de datos personales ha sido justamente el estar basado en una Directiva. La Directiva que será reemplazada por el Reglamento desde el 25 de mayo de 2018, no ha generado hasta la fecha una perfecta armonización de las leyes nacionales. Según se especifica en el preámbulo del Reglamento:

> Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en

---

y Libertades Fundamentales del Consejo de Europa, y por el artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea.

4. Primera parte dirigida por Marcel Moritz, MCF HDR.
5. CJCE, 14 de diciembre de 1971, aff. 43/71, Politi; CJUE, 10 de octubre de 1973, aff. 37/73, Fratelli Variola.

> particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal en lo que respecta al tratamiento de dichos datos en los Estados miembros, pueden impedir la libre circulación de los datos de carácter personal en la Unión.[6]

En el fondo, no es sorprendente que muchas disposiciones del Reglamento hayan sido copiadas directamente de la Directiva 95/46/CE. Tal es el caso, por ejemplo, del campo de aplicación material del texto,[7] ya que el Reglamento se aplica al tratamiento de datos personales automatizados, en todo o en parte, así como para los ficheros no automatizados. Pero no se aplica ni para la persecución y sanción de actividades delictivas, ni para la seguridad pública, ni para las actividades domésticas de un individuo.

Las principales definiciones[8] (datos personales, procesamiento, archivo, controlador, etc.) no contienen cambios significativos en comparación con la Directiva de 1995,[9] pues muchos de estos principios han sido transcritos de la Directiva. A modo de ejemplo, el contenido del artículo 5 del Reglamento sobre los principios para el tratamiento de los datos personales no causan sorpresa. Encontramos los principios de legalidad, imparcialidad, transparencia, la limitación, los objetivos, la minimización de datos, precisión, seguridad. Todos estos principios ya fueron instituidos en la Directiva de 1995, y ya constan en las leyes nacionales, en particular el artículo 6 acerca de la calidad de los datos.

Por lo tanto, debemos remarcar a título preliminar una precisión importante: a pesar de que el Reglamento contiene ciento setenta y tres (173) considerandos y noventa y nueve (99) artículos, no constituye un texto que sea en su mayor parte *inédito*. Gran parte de estas disposiciones han estado desde hace mucho tiempo plasmadas en el derecho positivo de los estados miembros de la Unión Europea. La doctrina tiende en consecuencia a limitar el aporte del Reglamento.

> Se detecta en el nuevo Reglamento de la UE, pocas novedades respecto a la orientación previa en la determinación de los derechos de las personas implicadas, y las obligaciones impuestas a los administradores de procesamiento de datos. La armonización europea de-

6. Cons. 9 del Reglamento.
7. Art. 2 del Reglamento.
8. Art. 4 del Reglamento.
9. Sin embargo, hay que tener en cuenta la introducción del concepto de seudonimización, definido en el art. 4 del Reglamento como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

> seada parece más inspirada por el deseo de promover "flujo transfronterizo de datos" entre Estados miembros –entre los cuales en general no existen límites. E incluso a terceros países, con iniciativas de refuerzo para la protección de datos.[10]

En este conjunto muy amplio que constituye la normativa, sí es posible destacar una serie de aportes importantes.

Innovaciones jurídicas con efectos antagónicos

La lectura de los ciento setenta y tres (173) considerandos del Reglamento permite comprender de mejor manera las finalidades del texto, las que podríamos resumir de la siguiente manera: "asegurar un nivel equivalente de protección de personas físicas, y la libre circulación de datos personales a través de la Unión".[11] Esta fórmula ilustra perfectamente el desafío que enfrenta el Reglamento, debiendo a la vez proteger los datos personales de los individuos, y la vitalidad del mercado único en el que estos datos son un recurso valioso.

En consecuencia, el resultado no solo es la afirmación de nuevos derechos para los individuos, sino también el surgimiento de oportunidades sin precedentes para las empresas que en gran medida prestaron su pluma para la redacción de este reglamento.[12] A continuación abordaremos ambos enfoques.

En cuanto a los nuevos derechos asignados a los individuos, el Reglamento refuerza la protección de los "niños",[13] ya que en el entorno de los servicios de la sociedad de la información[14] el consentimiento para un menor de 16 años (o 13 años si la ley del Estado miembro lo permite) debe ser lícito y autorizado por su representante legal.

Más allá de esta categoría específica de personas, el Reglamento instituye varias medidas de protección, particularmente el derecho a la supresión[15] de datos, igualmente calificado por el texto –para nosotros de manera un poco excesiva– como *dere-*

---

10. E. Derieux, "Protection des données à caractère personnel et activités de communication publique Apports du règlement européen du 27 avril 2016 au regard de la précédente directive du 24 octobre 1995 et de la loi française du 6 janvier 1978 (révisée par celle du 6 août 2004)", *Revue Lamy Droit de l'Immatériel*, No. 128 (2016): 15.
11. Cons. 170 del Reglamento.
12. V. especialmente: Y. Eudes, "Très chères données personnelles", en *Le Monde*, 2 de junio de 2013.
13. Art. 8 del Reglamento.
14. Definido conforme a la Directiva No. 98/34/CE: "todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios".
15. Art. 17 del Reglamento.

cho al olvido. Este derecho es aplicable cuando los datos ya no son necesarios, cuando la persona retira su consentimiento, cuando ejerce su derecho de oposición,[16] cuando el tratamiento es ilícito, o cuando la ley impone la supresión de datos en causa.

Entre los aportes significativos podemos citar la consagración de un derecho a la portabilidad de datos,[17] que permite a un individuo exigir la restitución en un formato explotable de los datos que hayan sido transmitidos al responsable del tratamiento automatizado de datos, o aquellos que hubiesen sido transmitidos directamente de un responsable del tratamiento a otro, siempre y cuando sea técnicamente posible. Sin embargo, esta disposición se reserva los derechos y libertades de terceros, por cuanto podrían limitar su aplicación en otras áreas jurídicas, como por ejemplo la propiedad intelectual.

El artículo 22 del Reglamento es igualmente interesante, por cuanto prohíbe –salvo excepciones– que una persona sea objeto de "una decisión basada únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produjeren efectos jurídicos en él, o le afecten de manera significativa de modo similar".[18] El futuro nos revelará cual es el significado preciso de estas disposiciones, las cuales bien podrían ser un límite importante para las actividades de algunas empresas, siempre y cuando una interpretación restrictiva no neutralice su potencial.

Además de las disposiciones enfocadas en proteger a los individuos, algunas de los cuales se acaban de describir brevemente, el Reglamento también establece en muchos aspectos cierta flexibilidad para los responsables del tratamiento. Como se subraya en la doctrina, "una de las principales diferencias entre la directiva de 1995 y el Reglamento radica en la reducción de cargas administrativas para los responsables del tratamiento de datos: las formalidades previas han sido eliminadas en la mayoría de los casos".[19] Es sobre la base de esta lógica que el Reglamento establece el mecanismo de análisis de impacto para tratamientos susceptibles de engendrar un riesgo elevado que afecte los derechos y libertades de las personas físicas,[20] el nombramiento de un delegado para la protección de datos,[21] o también el desarrollo de códigos de conducta[22] y mecanismos de certificación,[23] ambos fuertemente promovidos en el texto.

---

16. Este derecho de oposición está previsto por el art. 21 del Reglamento.
17. Art. 20 del Reglamento.
18. Art. 22 del Reglamento.
19. F. Mattatia, "Synthèse du futur règlement européen sur les données personnelles", *Revue Lamy Droit de l'Immatériel*, No. 126 (2016): 42.
20. Art. 35 del Reglamento.
21. Art. 37 y 39 del Reglamento.
22. Art. 40 y 41 del Reglamento.
23. Art. 42 y 43 del Reglamento.

En resumen, el Reglamento pone gran énfasis en la responsabilidad de los actores económicos que, se supone, deben estar más involucrados en el cumplimiento de sus tratamientos. Si bien es comprensible que "es importante, en particular, que el responsable del tratamiento esté obligado a implementar medidas adecuadas y eficaces, y ser capaz de demostrar que las operaciones son conformes a las establecidas en el presente Reglamento",[24] también es relevante preguntarse si es que asumir una forma de autocontrol podría ser peligroso. La ambigüedad del Reglamento podría abrir la puerta para posibles incertidumbres jurídicas.

UN REGLAMENTO FUENTE DE INCERTIDUMBRES JURÍDICAS[25]

La voluntad de asegurar un nivel excepcional de protección en los veintiocho (28) estados, pero sin comprometer el desarrollo de los mercados clave para la Unión, dio lugar a un texto ambiguo, que afecta tanto al alcance del texto (a), como su función unificadora del Derecho (b).

Un texto en el que el radicalismo frecuenta un enfoque basado en el riesgo

La primera parte de este estudio demostró que el Reglamento tiende a desarrollar un nivel muy elevado de protección, añadiendo nuevos derechos y obligaciones al edificio construido por la Directiva de 1995, los cuales son ahora directamente aplicables en los estados miembros.

La consagración de un "derecho al olvido" (art. 17),[26] el reconocimiento de un principio de minimización de los datos recogidos (art. 5-1, c), o la protección de datos desde el diseño (art. 25), así como penas más severas, bien podrían revelar una postura radical[27] en algunos de los redactores del Reglamento. Si bien, a priori, este enfoque pretender hacer de la Unión Europea un territorio excepcional de protección

24. Cons. 74 del Reglamento.
25. Segunda parte dirigida por Valentin Gibello, doctorante (CERAPS, UMR 8026).
26. De hecho, es una variación del derecho a la supresión de datos que ya incluía la directiva de 1995.
27. Sobre la concepción maximalista de la protección de derechos fundamentales, ver: E. Brems, "Droits humains, étrangers et multiculturalisme: pour une approche maximaliste et inclusive des droits fondamentaux", *Revue Trimestrielle des Droits de l'Homme*, vol. 82 (2010): 237-49.

del derecho a la vida privada, algunos ya están preocupados por la posibilidad de que el Reglamento no esté a la altura de sus propias ambiciones.[28]

Pero, sin prejuzgar los futuros efectos del Reglamento y de los méritos de este enfoque, es conveniente encontrar la esencia real del texto, con la finalidad de investigar su verdadero alcance más allá de la enunciación de principios. Sin embargo, una ambigüedad importante radica en la coexistencia, por un lado, del reconocimiento de un vasto conjunto de derechos y obligaciones, y por el otro, de la implementación de métodos de gestión de riesgos.

De esta manera, el responsable del tratamiento está obligado a proceder a la supresión de datos "teniendo en cuenta la tecnología disponible, y el coste de su implementación" (art. 17-2). Del mismo modo, los principios cardenales del Reglamento, el de responsabilidad (art. 24), de protección de datos desde el diseño (art. 25), o los de seguridad del tratamiento (art. 32), se ejercen "a la luz de su naturaleza, su alcance, su contexto y los propósitos del tratamiento así como sus riesgos, considerando que su nivel de probabilidad y gravedad varía de acuerdo a los derechos y libertades de las personas físicas".

Estas limitaciones, así como la importancia que el Reglamento otorga a las nociones de "responsabilidad" y "análisis de riesgos" (art. 35),[29] revelan la opción tomada por sus redactores de utilizar un enfoque de riesgos (risk-based approach), una opción que no es neutral para la protección efectiva del derecho fundamental a la vida privada.

Unánimemente adoptada por todas las delegaciones que contribuyeron a la elaboración del texto, y al tenor de los instrumentos de trabajo interinstitucionales,[30] el enfoque fundado sobre los riesgos es directamente una copia del modelo legislativo anglosajón. Desarrollado en el Reino Unido en los años 1990,[31] bajo la presión correguladora de las empresas, sobre todo del sector financiero, la cual permanece en el corazón de la política legislativa británica desde la New Labour.[32]

---

28. G. Desgens-Pasanau, "RGPD: entre incertitudes et occasions manquées", *Dalloz IP/IT*, No. 77 (2016): 335-9.
29. La cual debe contener "una evaluación de los riesgos para los derechos y libertades de los interesados [...]" y "las medidas previstas para afrontar los riesgos [...]".
30. Consejo de la Unión Europea, Secretaría General del Consejo, Archivo Interinstitucional 2012/0011 (COD), 2 de septiembre de 2014, Bruselas. Disponible en ‹http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012267%202014%20REV%202›. Consulta: 10 de enero de 2017.
31. Ver en M. Moran, "Understanding the Regulatory State", *British Journal of Political Science* 32, No. 2 (2002): 391-413.
32. Ver el reporte encargado por el Gobierno, P. Hampton, *Reducing administrative burdens: effective inspection and enforcement*, HMSO, 2005, cuyos principios han sido integrados en el Código Re-

Esta concepción de cómo hacer el Derecho presume el fracaso de las regulaciones clásicas, las cuales contemplaban una carga insoportable de formalidades para las empresas, y por lo tanto constituirían un impedimento importante para el desarrollo económico. Este elemento de discurso, que hizo consenso durante las negociaciones, es cuestionable por varias razones. En primer lugar, cabe considerar que la realidad misma de las potenciales economías[33] no es suficientemente establecida,[34] y el argumento es frecuentemente manejado por los grupos de presión a favor de una regulación "dúctil" y "flexible", en pocas palabras, menos restrictiva.

La transición hacia un enfoque basado en el riesgo es promovida por el Reglamento, incluyendo requisitos de documentación, y llevar a cabo evaluaciones de impacto, lo cual lógicamente incrementaría los costos de desarrollo.[35] Sobre la base de esta hipótesis, el *risk-based approach* recomienda dejar a los actores económicos modular la intensidad de sus obligaciones, de acuerdo a los riesgos de una actividad dentro de un contexto definido.

Traducido al derecho a la protección de datos personales, esto significa que será necesario que el responsable de un tratamiento de datos que presente riesgos elevados que atenten contra el derecho de la vida privada de las personas, esté obligado a invertir más recursos para su cumplimiento (mayor seguridad, protección de datos por diseño, nombrar a un RPD, análisis de impacto, etc.).

En contraste, el tratamiento de datos con menor riesgo conlleva a un menor peso de obligaciones para el responsable del tratamiento. ¿Es tal enfoque realmente adaptable a la protección de un derecho fundamental como es el derecho a la vida privada? En nombre del pragmatismo, ¿ha cedido el Reglamento ante grupos de poder comprometiendo la posibilidad de llegar a establecer una protección eficaz y uniforme del derecho a la vida privada en la Unión?

Podemos preocuparnos acerca de si este método es adecuado para asegurar la protección del derecho individual a la vida privada, al no involucrar al Estado.[36] El cumplimiento basado en el riesgo deja que los responsables del tratamiento evalúen los

---

gulador. Disponible en ‹https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/300126/14-705-regulators-code.pdf›. Consulta: 10 de enero de 2017.

33. 2,3 millones de euros de economía para los actores económicos, según la Comisión, ver: London Economics, *Implications of the European Commission's proposal for a general data protection regulation for business - Final report to the Information Commissioner's Office*, mayo de 2013, vii.
34. Lo demuestran las conclusiones del informe de la agencia de protección de datos inglesa, l'ICO, ibíd.
35. Los "*compliance costs*", como se destacó por parte de la delegación holandesa en el mencionado documento de trabajo: Council of the European Union, 97.
36. Recordando el rol principal del Estado en la protección del derecho a la vida privada: J. J. Lavenue,

riesgos de las personas afectadas, a pesar de que el enfoque de riesgos tal como se utiliza en todas otras áreas, consiste en identificar los riesgos para la propia empresa y responder con los recursos disponibles. Determinar los riesgos de la privacidad de las personas afectadas es un asunto discutido, pero no sin consecuencias. De hecho, los riesgos son diferentes en su naturaleza y el alcance de manera individual, y cada persona tiene la facultad de determinar los límites de su vida privada.[37]

Es también lamentable que el Reglamento se fundamente en la búsqueda de un compromiso entre el derecho a la vida privada y las prioridades económicas de las empresas. Si bien es necesario establecer un equilibrio, este debería ser entre el derecho fundamental específico y otros derechos fundamentales con los cuales podría entrar en conflicto, incluida la libertad de expresión o el derecho a la información. En términos más generales, podemos evaluar este cambio como una transición sutil del derecho a la vida privada, hacia un derecho a la *privacy*, y su lógica anglosajona de carácter mercantil, que sugiere la vacilación constante entre el Reglamento y el enfoque patrimonial y extra patrimonial de la noción sobre los datos de carácter personal.[38]

Acerca de las objeciones presentadas en contra de este método, el grupo de trabajo del artículo 29 (G29) tuvo la precaución de contestar el 30 de mayo de 2014,[39] destacando por encima de todo, lo que ya estaba presente en la Directiva de 1995.[40] Sin embargo, el G29 defiende un diseño totalmente diferente al de las fuerzas del *lobbying*, y considera al enfoque basado en el riesgo como la forma de *aumentar* las obligaciones del responsable del tratamiento de riesgos, aplicando lo mismo para los tratamientos que juzga como "de bajo riesgo".[41]

Además de estar –a partir de ahora– impuesto a los estados miembros, y generalizado en todo el derecho de protección de datos, el enfoque basado en el riesgo que irriga el Reglamento, no logró de alguna manera disuadir los votos de la G29. Está previsto por ejemplo, que las obligaciones ante cualquier violación de los datos personales (art. 33 y 34) no se apliquen a los tratamientos de bajo riesgo. Dada la falta

---

C. Codron, N. Desrumeaux y G. B. Hamerel, "Privacy by design ou Privacy by law", *Revue Droit international, Commerce, Innovation et Développement*, No. 2 (2012): 77-104.

37. Ver sobre este punto: B. Beigner y J. Antippas, "La protection de la vie privée", en *Libertés et droits fondamentaux* (París: Dalloz, 2015), 239.
38. Sobre esta diferencia, ver: C. Wolf y M. Winston, "So Close, Yet o Far Apart: The EU and US Visions of a New Privacy Framework", *Antitrust* 26, No. 3 (2012).
39. Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", No. 14/EN WP 218, adoptado el 30 de mayo de 2014.
40. Principalmente en las obligaciones de seguridad de datos del art. 17.
41. Art. 29 Data Protection Working Party, ibíd.

de definición del concepto de "riesgo" en el Reglamento,[42] ya se puede cuestionar el alcance real de muchos de los derechos y obligaciones establecidos.

En la práctica, las consecuencias para la protección de la vida privada dependerán del equilibrio necesario entre el deseo de pragmatismo que promueva el control a posteriori, de los mecanismos de regulación menos verticales, y la fuerza vinculante del Reglamento, que representan el aumento de las sanciones y la supervisión del rol de las agencias de protección de datos. Otra ambigüedad mayor será la capacidad de armonizar el derecho de este Reglamento Europeo, directamente en peligro por su contenido mismo.

Una voluntad de armonización contradicha en el texto

De hecho, a pesar de la extrema longitud del texto (173 considerandos, 99 artículos) y las redundancias que contiene, persisten muchas incertidumbres cuya resolución necesita de un trabajo consistente de interpretación.

En primer lugar, los estados pueden introducir en diversos entornos, normas nacionales diferentes a las del Reglamento, en el sentido de una mayor protección de las personas afectadas. Las disposiciones relativas al tratamiento de los datos biométricos son un ejemplo notable, tomando en cuenta el gran crecimiento de su utilización (seguridad de pagos, lucha contra el terrorismo, identidad digital).

Desde el punto de vista económico, el Reglamento se aplica para establecer un régimen *a minima*, según el cual los datos biométricos adoptan la calificación de los datos sensibles en el sentido del artículo 9, y, por lo tanto, su tratamiento está en principio prohibido. Este principio de prohibición va acompañado inmediatamente de una decena de excepciones, incluyendo el consentimiento explícito de la persona interesada. En este punto, el Reglamento ya admite que la legislación nacional de un Estado miembro pueda neutralizar dicha excepción.[43]

Además de obtener el consentimiento, el responsable de un tratamiento de datos biométricos deberá, a priori, cumplir con el procedimiento de "consulta previa" sobre la base del análisis de impacto requerido por el artículo 36 e interpretado por el delegado de protección de datos, cuyo nombramiento se hace entonces obligatorio (art. 37). Esto sin tomar en cuenta el artículo 9-4, que añade: "Los Estados miembros podrán mantener o establecer condiciones adicionales, incluyendo limitaciones, en

42. A lo sumo, el considerando 75 establece algunas indicaciones.
43. Art. 9-2, a) del Reglamento.

cuanto al tratamiento de datos genéticos, datos biométricos o datos relativos la salud". En otras palabras, los legisladores nacionales pueden añadir otros requisitos, tales como, prohibir por completo el procesamiento de datos biométricos.

Esta disposición lejos de ser una oportunidad para mejorar la protección del derecho a la vida privada en relación a los riesgos del uso de la tecnología, conlleva a renunciar al efecto de la unificación del Derecho propio de este instrumento. La capacidad de la Unión Europea para edificar un frente común en materia de protección de datos personales condiciona directamente la efectividad de esta protección. Por otra parte, una flexibilidad de tal magnitud allana el camino para la adopción de disposiciones nacionales imprecisas y ambiguas, como es el caso de las iniciativas francesas recientes.[44]

Además de estas disposiciones sobre la biometría, existe la posibilidad de que los estados miembros se desvíen del Reglamento con respecto a las reglas de licitud del tratamiento (art. 6), las disposiciones aplicables al trabajo (art. 90), la definición de tratamiento que requiere de una evaluación de impacto (art. 35-3), el uso del número de identificación nacional (art. 87), o la edad de consentimiento para menores al tratamiento de sus datos (art. 8-1).

Por otra parte, el Reglamento es objeto de críticas tanto de representantes y especialistas de la industria digital, en cuanto la falta de precisión de ciertas nociones[45] cuya importancia operativa es grande. Así que ¿cuáles son los criterios para evaluar la noción de "alto riesgo", que se utiliza en varios lugares de la conciliación? ¿Desde qué momento es implementado un tratamiento de datos "a gran escala", e impone nuevas responsabilidades al responsable del tratamiento? ¿Se pretende aplicar el derecho al olvido establecido en el artículo 17 a los motores de búsqueda, en la línea que marcó la sentencia del 13 de mayo de 2014 en el caso de Google España?[46] ¿Cuál es el perímetro del nuevo derecho a la portabilidad de los datos establecido en el artículo 20?

---

44. De hecho, la aprobación en el Senado de la ley "*pour une République numérique*" vio un nuevo intento de introducir medidas restrictivas para el tratamiento de datos biométricos, los cuales, mal concebidos, conllevarían en definitiva a bajar el nivel de protección de los franceses con respecto a la biometría, dicha "*de service*".
45. Tomaremos como prueba las contribuciones a la consulta abierta por la CNIL en vista de los trabajos para la aplicación del Reglamento en 2018. Ver la síntesis en esta dirección: ‹https://www.cnil.fr/sites/default/files/atoms/files/resultats_de_la_consultation_publique_reglement_0.pdf›. Consulta: 11 de enero de 2017.
46. CJUE, grande chambre, 13 de mayo de 2014, *Google Spain SL*, C-131/12. E. Brunet, "Règlement général sur la protection des données à caractère personnel-Genèse de la réforme et présentation globale", *Dalloz IP/IT*, No. 12 (2016): 567-72.

CONCLUSIONES

El Reglamento Europeo (UE) 2016/679 deja muchas interrogantes que requerirán de un largo trabajo de interpretación, lo que determinará su alcance real y su función armonizadora. El riesgo es que este trabajo se realice en primer lugar a nivel nacional y que se mantengan las diferencias en los enfoques que existían entre las agencias europeas de protección de datos en el ámbito de la Directiva de 1995. No obstante, la duda permanecerá acerca de su capacidad para lograr una concepción unificada y protectora del derecho a la vida privada en todos estos puntos, mediante el establecimiento del Comité Europeo de Protección de Datos creado en el artículo 68.

Cabe agregar que el equilibrio de este nuevo marco legal se fundamenta en la disuasión y el carácter verosímil de las sanciones que proporciona. Está diseñado para evitar abusos en la aplicación del principio de la responsabilidad y la lógica de control a posteriori. Por otro lado, existen pocas garantías para protegerse contra las diferencias excesivas en la aplicación de sanciones económicas por parte de las agencias de protección de datos. No hay ninguna indicación de que el Reglamento pondrá fin a la situación actual, en la cual coexisten en la Unión Europea algunas agencias reacias, como es la CNIL francesa,[47] o, por el contrario, más flexibles como la Agencia Española de Protección de Datos (AEPD).

Aparte de las sanciones, el Reglamento se apoya fuertemente en el proceso de certificación (etiquetas, códigos de conducta), que constituyen de igual manera una clave para la aplicación efectiva del principio de protección de datos. No obstante, podemos dudar de las posibilidades de lograr una política armonizada en la materia, por cuanto la regulación mantiene un nivel de certificación nacional (art. 42).

De manera más general, por la falta de éxito de la certificación nacional hasta el momento, y la falta de incentivo real para usarlo en la regulación, la armonización de la política de certificación podría incluso llegar a ser un asunto secundario.[48]

El nuevo Reglamento General sobre la protección de datos, que estará vigente a partir del 25 de mayo de 2018, la ley común de la Unión Europea en esta materia, está

---

47. Según el reporte anual de 2016, solamente tres sanciones pecuniarias han sido pronunciadas por la CNIL, que prefiere un enfoque pedagógico basado en gran parte sobre la actividad informática correspondiente y las libertades, que reemplazarán al *oficial de protección de datos*.
48. Sobre este punto, ver: O. Tambou, "L'introduction de la certification dans le règlement général de la protection des données personnelles: quelle valeur ajoutée?", *Revue Lamy droit de l'immatériel* 5, No. 126 (enero 2016): 43-48; E. Lachaud, "Why the certification process defined in the General Data Protection Regulation cannot be successfu", *Computer Law & Security Review* 32, No. 6 (diciembre de 2016): 814826.

impregnado de tantas ambigüedades como ambiciones. Una lectura profunda de sus numerosas disposiciones, altamente protectoras a priori del derecho fundamental a la vida privada, revela un pragmatismo de concesiones hechas a los actores económicos. Será misión de las instituciones de protección de datos nacionales y europeas, el encontrar la manera de evitar abusos a través de un arduo trabajo de interpretación en la práctica.

BIBLIOGRAFÍA

Beigner, B., y J. Antippas. "La protection de la vie privée". *Libertés et droits fondamentaux*. Paris (2015).

Brems, E. "Droits humains, étrangers et multiculturalisme: pour une approche maximaliste et inclusive des droits fondamentaux". *Revue Trimestrielle des Droits de l'Homme*, vol. 82 (2010).

Derieux, E. "Protection des données à caractère personnel et activités de communication publique Apports du règlement européen du 27 avril 2016 au regard de la précédente directive du 24 octobre 1995 et de la loi française du 6 janvier 1978 (révisée par celle du 6 août 2004)". *Revue Lamy Droit de l'Immatériel*, No. 128 (2016).

Desgens-Pasanau, G., "RGPD: entre incertitudes et occasions manquées". *Dalloz IP/IT*, No. 7 (2016).

Lachaud, E., "Why the certification process defined in the General Data Protection Regulation cannot be successful". *Computer Law & Security Review* 32, No. 6 (2016).

Lavenue, J.-J., C. Codron, N. Desrumeaux y G. B. Hamerel. "Privacy by design ou Privacy by law". *Revue Droit international, Commerce, Innovation et Développement* (2012).

London Economics. *Implications of the European Commission's proposal for a general data protection regulation for business - Final report to the Information Commissioner's Office*, 2013.

Mattatia, F. "Synthèse du futur règlement européen sur les données personnelles". *Revue Lamy Droit de l'Immatériel*, No. 126 (2016).

Wolf, C., y M. Winston. "So Close, Yet o Far Apart: The EU and US Visions of a New Privacy Framework". *Antitrust* 26, No. 3 (2012).

Fecha de recepción: 7 de febrero de 2017
Fecha de aprobación: 31 de mayo de 2017

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

Protección de datos personales y derecho al olvido. Análisis del caso Perú *vs.* Google

*Alexander Cuenca Espinosa**

RESUMEN

El presente artículo está orientado al análisis del recurso de reconsideración planteado por el recurrente (Google Perú SRL) en el caso Perú *vs.* Google, por cuanto el reclamante denuncia la no cancelación de datos personales, respecto a un sobreseimiento, que afecta su imagen pública, en contra de Google Perú SRL, cuando este último no efectúa actividad alguna que tenga relación con la indexación de información en los motores de búsqueda, ya que dicha labor es de responsabilidad de Google Inc. domiciliada en EE. UU., a la cual no le llega notificación legal alguna, dejándola en estado de indefensión. En este ámbito, también se refiere a la resolución sancionatoria, que, si bien considera los derechos ARCO respecto al titular de la acción, no toma en cuenta el derecho a la defensa del recurrente y la libertad de expresión.

Palabras clave: protección de datos personales, buscadores en internet, google, cibernética, libertad de expresión.

ABSTRACT

The main objective of this article is aimed at analyzing the appeal of reconsideration raised by the appellant (Google Peru SRL) in the case of Peru *vs.* Google, reason why the complainant denounces the non-cancellation of personal data, which affect its public image against Google Perú SRL, when the latter does not carry out the activity that has to do with the indexing of information in search engines, since that is the work of Google Inc. resident at EE. UU. To which no legal notice arrives, leaving it in a state of defenselessness. In this area, it also refers to the sanctioning resolution while considering ARCO rights with respect to the owner of the action, does not take into account the right to defend the recurrence and freedom of expression.

Keywords: data protection, search engines, google, cybernetics, freedom of speech.

* Docente de la Maestría en Seguridad y Riesgo de la Universidad de las Fuerzas Armadas, ESPE.

Cuando se descubrió que la información era un negocio,
la verdad dejó de ser importante.

Ryszard Kapuscinski

INTRODUCCIÓN

El presente artículo pretende analizar el recurso de reconsideración presentado por Google en el caso Perú *vs.* Google, correspondiente a las responsabilidades atribuidas sobre la protección de datos personales y el derecho al olvido respecto a la información indexada dentro del motor de búsqueda de Google.

Antes de comenzar, se debe señalar que, si bien la mayoría de países en Latinoamérica goza de una legislación penal que castiga los delitos que atenten contra la divulgación de información privada y protegida, pocos son los países que tratan la temática de protección de datos personales con una legislación propia, separando la sanción administrativa de la sanción penal. Entre estos países tenemos: Argentina, Uruguay, México, Colombia, Perú y Nicaragua. En el caso de Ecuador, en el año 2016 se presentó un proyecto de ley para tratar esta temática, sin embargo, por no tener el apoyo suficiente de la bancada legislativa, este proyecto fue archivado.

ANTECEDENTES

Sobre el caso concreto, el conflicto nace porque Google no atiende debidamente el reclamo donde el afectado solicita la eliminación de un contenido relacionado con una causa judicial que aparecía en los resultados indexados en los motores de búsqueda pertenecientes a Google Perú.

La razón de la reclamación radica en la afectación que el solicitante considera tener sobre su derecho al honor y buen nombre, por cuanto la población internauta suele considerar totalmente veraz un contenido sin verificarlo previamente, y a base de este procede a hacer sus juicios de valor respecto a una persona, que en el presente caso afectaría no solo a su autoestima sino también en asuntos socioculturales externos.

En esta órbita, el reclamante hace hincapié en la aplicación del derecho al olvido, por cuanto cabe recalcar que este es un derecho que surge en el empleo de nuevas tecnologías, concretamente el internet, como atañe el caso de análisis, considerándolo como derivativo del derecho a la intimidad. Así lo refiere Luis Mieres cuando manifiesta que "del derecho a la intimidad puede derivarse un derecho

al olvido"[1] describiendo que este último se aplica cuando "un dato que ha sido público, por el trascurso del tiempo, trasmuta su calidad y deviene en privado o íntimo".[2] Es decir, el usuario afectado con esto requiere que los datos que circulan en el motor de navegación del internet, pese a haber sido de acceso a todos los internautas, se eliminen del mismo, para evitar a partir del este acto, su acceso a la sociedad toda, protegiendo no solo su derecho a la intimidad, sino el del honor y buen nombre.

Por esto, el reclamo fue presentado el 7 de octubre de 2015, ante la Dirección General de Protección de Datos Personales del Perú, que resolvió el reclamo mediante Resolución Directoral número 045-2015-JUS/DGPDP, el 30 de diciembre de 2015, ordenando a Google Perú el bloqueo de la información que contenía los datos del reclamante en un término de diez días, y de informar en los cinco días subsiguientes a este término sobre la medidas de cumplimiento que adoptó para bloquear este contenido.

Al respecto, cabe mencionar que la Dirección General de Protección de Datos Personales de Perú, al tener conocimiento del caso, "declaró fundada la reclamación", tomando en cuenta exclusivamente la argumentación efectuada por el solicitante, sancionando de manera directa y estableciendo fechas para el cumplimiento de la sanción, razón por la cual incurre en error judicial por cuanto no tienen la oportunidad de valorar la prueba de la contraparte, denegando de cierto modo el acceso a la justicia.

Así pues, de la orden para el bloqueo y eliminación de datos personales del afectado, la Dirección General de Protección de Datos Personales del Perú sancionó a Google Perú con treinta y cinco unidades impositivas tributarias por no atender la solicitud del titular, lo que equivale en Ecuador a cuarenta y tres dólares; y con treinta unidades impositivas tributarias (treinta y siete dólares) por desconocer los derechos de cancelación y oposición.[3]

Sobre esta primera parte, me permito hacer una breve crítica. Si bien la sanción administrativa es adecuada porque se le ordena el bloqueo de la información perjudicial en un tiempo determinado, la sanción pecuniaria no es la correcta, puesto que la honra, la moral y la intimidad de una persona no tienen precio; por consiguiente, su cuantía es muy cuestionable y discutible a la vez, partiendo del hecho que toda persona ante los DD HH goza de igualdad de derechos, debemos denotar que en la sociedad en la que vivimos se tiende a sobrevalorar a una persona por su profesión y popula-

1. Luis Mieres, *El derecho al olvido digital* (Cataluña: Iosu Latorre, 2014), 13.
2. Ibíd.
3. Conocidos también por sus siglas como derechos ARCO.

ridad en un sector determinado; ahora, sobre el caso analizado, el afectado inicia un reclamo porque se afecta a su persona con información que se encuentra en el motor de búsqueda en relación a una causa judicial; como sabemos, una causa judicial puede afectar en mucho a la reputación de una persona, ya que puede contener información sobre un delito que se le imputa. Es así que la multa impuesta a Google Perú es poco significativa en relación al bien jurídico afectado.

SOBRE EL RECURSO DE RECONSIDERACIÓN

Google Perú SRL interpone el recurso de reconsideración por los siguientes motivos:

- Legitimación de personería: el recurrente indica que la denuncia debió haber sido planteada en contra de Google Inc., mas no en contra de Google Perú SRL, pues sus potestades son diferentes. En el caso de Google Inc., su actividad comercial se relaciona al manejo y administración de cuentas de correo electrónico y al tratamiento de datos indexados en su motor de búsqueda, mientras que Google Perú SRL tiene el control de los productos y servicios de publicidad web que brinda dentro del territorio peruano.
- Notificación: la notificación en particular se la debe hacer en el domicilio civil de la persona jurídica con competencia de conocimiento y contestación; en el caso de Google Inc., esto es en Estados Unidos, en tal razón se incumple con esta formalidad, puesto que únicamente se lo notifica mediante un correo electrónico invalidado para tal motivo, afectando al debido proceso.
- Aplicación de tratados o convenios: la Dirección General de Protección de Datos Personales del Perú no aplica la Convención Interamericana sobre Cartas Rogatorias y Exhortos.
- Actividad persona jurídica: la Dirección General de Protección de Datos Personales del Perú busca responsabilizar a Google Perú SRL sobre productos o servicios que no controla, como es la información indexada en los motores de búsqueda de Google Inc.
- Responsabilidad: las obligaciones impuestas a Google Perú SRL son de imposible cumplimiento, ya que las actividades que realiza esta persona jurídica en Perú, nada tienen que ver con el tratamiento de datos personales vinculados a actividades del buscador web de Google Inc.

Además de las expuestas anteriormente, Google SRL hace referencia a un correo electrónico enviado por la Dirección General de Protección de Datos Personales del Perú, en el que se presenta la denuncia sin seguir el canal respectivo. En este correo,

Google Inc. en los Estados Unidos le menciona que el correo electrónico enviado por la Dirección General de Protección de Datos Personales es inválido y no reconocido en los EE. UU., puesto que para su aplicabilidad se deben seguir varios acuerdos internacionales de cooperación jurisdiccional.

Sobre este último punto, es importante mencionar que las actuaciones realizadas por la Dirección General de Protección de Datos Personales del Perú, desde el punto objetivo del derecho carecen de validez, ya que como afirma Google Perú SRL, se violenta el derecho al debido proceso, puesto que se incumplen varias formalidades procesales necesarias para proseguir con el reclamo e imponer una sanción.

ARGUMENTOS DE LA DEFENSA

Google Perú SRL en defensa de sus propios derechos y de Google Inc., expone como argumentos:

- Aunque se haya notificado válidamente a Google Perú SRL en Lima, no se lo hizo a Google Inc. en el Estado de California en los Estados Unidos, conociendo que Google Perú SRL y Google Inc. son dos personas jurídicas distintas.
- Utilizar el domicilio local de Google Perú para notificar a una empresa extranjera totalmente distinta, como lo es Google Inc, convierte a la notificación nula de pleno derecho. Así, con este antecedente, Google Inc. no pudo ejercer el derecho a la defensa, pues no ha sido notificado de forma debida y legal en su domicilio personal.
- Se considera inadmisible que la Dirección General de Protección de Datos Personales del Perú intente notificar a una empresa extranjera a través de correo electrónico.

Por lo tanto, en relación a los puntos expuestos, la notificación es nula, lo que impide emitir un pronunciamiento respecto a la indexación de datos personales en el motor de búsqueda de Google. Adicionalmente, la falta de una correcta notificación vicia el procedimiento, pues no se da a conocer del hecho, circunstancia o acto del que se le acusa o amonesta; por esto de principio se atenta al debido proceso, al derecho a la defensa y a las garantías procesales básicas establecidas no solo en la legislación peruana, sino también en las convenciones y tratados internacionales, por ende, cualquier pronunciamiento de la Dirección General de Protección de Datos Personales del Perú carece de validez.

Es menester recordar que los tratados internacionales ayudan a la cooperación de los países para resolver problemas suscitados fuera de la jurisdicción mediante la asistencia judicial internacional.

CUESTIONAMIENTOS CON RELACIÓN AL TRATAMIENTO DE DATOS QUE EFECTÚA GOOGLE INC.

Google expone cuatro motivos sobre el tratamiento de datos, previo a que un reclamo sea presentado. En primera instancia, se deben considerar y corroborar que las URL o links que supuestamente afectan al reclamante, en efecto tengan material que pueda atentar contra su persona. En segundo lugar, menciona que previo al bloqueo de uno o varios links, el reclamante debe haber notificado con antelación a los administradores, webmasters y titulares de estos sitios web, a fin de que puedan ejercer su derecho a la defensa sobre el reclamo en cuestión. Como tercer punto, se considera que se debe escuchar a todas las partes por igual, incluidos los webmasters, administradores y titulares de los sitios web, puesto que de no hacerlo se transgreden derechos. Finalmente manifiesta que hay que considerar que los motores de búsqueda funcionan como facilitadores de información o meros intermediarios, por lo que la información gestionada, editada y redactada es responsabilidad de terceros y no de Google.

Sobre estos cuestionamientos es necesario precisar varios puntos: 1. Los buscadores electrónicos sea Google, Yahoo o Bing, lo que hacen es recopilar información de la web que facilita la búsqueda a los internautas. 2. Antes de precisar un reclamo a un buscador web en lo que respecta al derecho al olvido, lo ideal es ponerse en contacto con el sitio web que almacena el contenido objeto de reclamo. 3. En el presunto caso podría darse un reclamo contra Google, si este ha almacenado en su caché web[4] una vista previa del sitio web que vulnera derechos.

EL DERECHO A LA DEFENSA FRENTE AL DERECHO DE HONOR Y BUEN NOMBRE EN EL RECURSO DE RECONSIDERACIÓN

Para referirnos a este aspecto en concreto es importante tomar en consideración que todos los derechos tienen igual valor, sin embargo al momento de decidir, se debe tomar en consideración el derecho que ha sufrido mayor afectación.

4. Se conoce como caché web a los datos, documentos e imágenes almacenados por el motor de búsqueda de forma temporal.

Así, en el presente caso encontramos que se enfrentan dos derechos: el del honor y buen nombre –que es al que apela el reclamante– y el derecho a la defensa citado por la parte recurrente en el recurso.

En este sentido, Soria define al honor y buen nombre como "el crédito moral o manera en que se rinde frente a los demás y un plano valorativo del individuo frente a sí mismo".[5] Es decir, nos habla del honor y buen nombre como dualidad, en la que el individuo se considera en cuanto a su comportamiento respecto a el, generando una crítica constructiva y tomando en consideración la opinión que tiene respecto a sus actos la sociedad que lo rodea. Yendo de lo particular a lo general.

Por otro lado, en cuanto al derecho a la defensa, Gimeno Sendra se refiere a su fundamento manifestando que este "no es otro, sino el del propio principio de contradicción, el cual resulta ser consustancial a la idea de proceso".[6] Lo cual significa que es la oportunidad que se le da a la parte contraria para que a través de argumentos y las pruebas de las que se considere asistida demuestre que no tiene responsabilidad respecto de lo que se le acusa; esto a fin de evitar errores en la administración de justicia.

De este modo, se considera que para poder tomar una decisión es necesario adoptar un principio general, el de la ponderación, considerado como aquel "examen de proporcionalidad que busca establecer si el fin de cierta medida es lo suficientemente importante, en consideración al valor que el orden constitucional otorga al derecho que esta medida afecta".[7] Dicho en otras palabras, se considera en qué medida la aplicación de un derecho puede causar agravio al otro.

En el caso que nos atañe, si bien se puede evidenciar que el derecho de mayor afectación es el del honor y buen nombre, no es posible sancionar a una parte que no tiene responsabilidad alguna del acto que se le acusa, por tanto se debió haber tomado con mayor consideración el derecho a la defensa, que es el derecho que sufre la vulneración directa por la decisión emitida de la Dirección General de Protección de Datos Personales del Perú.

---

5. Carlos Pablo Márquez, *El delito informático conforme con el nuevo código penal. La información y la comunicación en la esfera penal* (Bogotá: Leyer, 2007), 59.
6. Faustino Gutiérrez, *El derecho a la defensa y la profesión de abogado* (Barcelona: Atelier, 2012), 31.
7. Eduardo Montealegre, *La ponderación en el derecho* (Bogotá: Universidad Externado de Colombia, 2014), 17.

CUESTIONAMIENTOS CON RELACIÓN AL EJERCICIO DE LOS DERECHOS ARCO (ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN)

Sobre los cuestionamientos de los Derechos ARCO, debemos tomar en consideración lo siguiente:

- De darse una presunta responsabilidad, esta podría ser de carácter vinculante, ya que no solo el buscador de Google Inc. indexa información para la búsqueda de datos, sino también otros motores de búsqueda como Yahoo, Bing, etc.
- Si bien la información puede ser indexada a los buscadores, los titulares de los contenidos, que en este caso son los sitios web que almacenan esta información, poseen las herramientas para que ciertos datos no aparezca en los motores de búsqueda de los navegadores, por lo tanto, la responsabilidad es exclusiva de los titulares de estos sitios.
- Los desarrolladores web tienen la capacidad y posibilidad de utilizar los llamados robots.txt y metatags para hacer visible cierta información, por lo que Google no tiene un control total sobre la información que se publica e indexa a su motor de búsqueda, es claro que los administradores de los sitios web y desarrolladores web pueden evitar que el contenido de estos sitios web se propague en el internet. Sin embargo, la operación técnica de asignar palabras que constituyan criterios de búsqueda es responsabilidad de los buscadores.

Así pues, se denota que el contenido expuesto claramente puede ser desvinculado de los buscadores web siempre que los administradores de estos contenidos utilicen las herramientas necesarias que eviten la propagación de información que pueda de manera indirecta violentar derechos, tal como las resoluciones judiciales de las personas, que como bien se lo menciona anteriormente, puede afectar la intimidad, la honra, el buen nombre y otros aspectos que conciernen a los derechos personalísimos.

CUESTIONAMIENTOS CON RELACIÓN A LA LIBERTAD DE EXPRESIÓN

La Dirección General de Protección de Datos Personales del Perú, a través de su potestad titular, de manera indirecta busca censurar la información contenida en los buscadores web, vulnerando el derecho a la libertad de expresión, sin antes hacer un juicio valorativo sobre el contenido de fondo de los links o URL que solicitan ser bloqueados; únicamente busca beneficiar al reclamante, solicitando a los intermediarios

de internet –en este caso Google– que bloqueen y hasta eliminen información que está fuera de su dominio, cuando se ha hecho énfasis que solo facilitan la búsqueda de información en la web al internauta.

Es claro que las potestades de la Dirección General de Protección de Datos Personales del Perú se extralimitan a ordenar situaciones que se encuentran fuera del alcance de Google, y que a su vez coartan el derecho de la libertad de expresión.

CONCLUSIONES FINALES DEL RECURSO DE RECONSIDERACIÓN

- Si bien los nombres de Google Inc. y Google Perú SRL parecen relacionarse, la Dirección General de Protección de Datos Personales del Perú debe diferenciar la personalidad jurídica que mantiene cada una de estas entidades, ya que sus fines societarios y comerciales son diferentes.
- El derecho del cual el reclamante debió asistirse para su solicitud es concretamente el derecho al olvido digital, que está relacionado con el derecho al honor y buen nombre y el derecho a la intimidad, por cuanto su objetivo radica en que se eliminen datos de acceso público de un motor de búsqueda en internet.
- El derecho al olvido debe considerarse como la posibilidad de retornar de un estado de datos personales publicados en internet, a un estado de ocultación plena y retorno a la intimidad de dichos datos, para sobre guardar el honor y buen nombre del interesado.
- El derecho al honor y buen nombre es el que sufre mayor afectación cuando datos personales se convierten en datos de acceso público en el internet.
- La notificación a Google Inc. debe cumplir con las solemnidades procesales necesarias para no atentar en contra del debido proceso, esto es la notificación en observancia de los convenios y tratados ratificados por ambos países en relación a la cooperación judicial internacional, y no por medio de un simple correo electrónico.
- De darse el no pago, puede haber una grave repercusión de carácter pecuniario que afectaría a Google Perú SRL mediante un juicio coactivo, sanción interpuesta por la Dirección General de Protección de Datos Personales del Perú.
- Se debe entender que Google Perú SRL no controla, ni administra, o aun peor realiza el tratamiento de datos vinculados a la información indexada en el buscador web de propiedad de Google Inc.

- No se puede limitar a responsabilizar a Google Inc. o en su defecto a Google Perú SRL por la información que se encuentra en la red, pues estos son meros intermediarios y facilitadores de los contenidos expuestos por ciertos sitios web.
- La responsabilidad directa se la debe seguir en contra del usuario que publica determinado contenido materia de la ilicitud dentro de un sitio web, blog o foro, por lo tanto, la responsabilidad administrativa debe ser ejercida en contra de estos.
- Al sancionar al recurrente con una injusta multa, se pretende, a más de levantar un precedente, el coartar la liberta de expresión, contraviniendo los derechos básicos dentro de las libertades que tiene el hombre, como bien se menciona en los argumentos expuestos por Google Perú SRL por sus propios derechos y en nombre de Google Inc.

Por último, los cuestionamientos y argumentos presentados por Google Perú SRL en representación de su intereses, nos conlleva a interpretar dos cosas: 1. Google Inc. a través de Google Perú SRL hace uso de su derecho a la defensa manifestando que la notificación se ha tramitado de manera incorrecta, omitiendo las solemnidades circunstanciales para este acto, esto es a través de la cooperación judicial internacional. De esta manera, libera a Google Inc. de cualquier responsabilidad. 2. Google Perú SRL, por otra parte, deja constancia en sus argumentos de defensa que no tiene vinculación alguna con el motor de búsqueda de Google Inc, y que la responsabilidad de esta no está ligada a su empresa. Por lo tanto, es inaplicable una sanción pecuniaria hacia una entidad que nada tiene que ver con la información indexada en el motor de búsqueda de Google Inc, en cuanto no le corresponde manifestarse sobre los derechos ARCO.

Finalmente, la Dirección General de Protección de Datos Personales del Perú resuelve declarar de infundado el recurso de reconsideración planteado por Google Perú SRL o en su defecto Google Inc. ratificando la sanción y condenando al pago dentro de los diez días hábiles a partir de la emisión de la resolución.

BIBLIOGRAFÍA

Gutiérrez, Faustino. *El derecho a la defensa y la profesión de abogado*. Barcelona: Atelier, 2012.

Márquez, Carlos Pablo. *El delito informático conforme con el nuevo código penal. La información y la comunicación en la esfera penal*. Bogotá: Leyer, 2007.

Mieres, Luis. *El derecho al olvido digital*. Cataluña: Iosu Latorre, 2014.

Montealegre, Eduardo. *La ponderación en el derecho*. Bogotá: Universidad Externado de Colombia, 2014.

Otros

República del Perú. *Resolución Directoral No. 026-2016-JUS-DGPDP*. Lima: Dirección General de Protección de Datos Personales, 2016.

Fecha de recepción: 18 de febrero 2017
Fecha de aprobación: 3 de mayo de 2017

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

El derecho al olvido en la era digital. El caso de Google en España y El Tiempo en Colombia

*María Gabriela Espinoza**

RESUMEN

La Corte Europea de Justicia en el caso Google *v.* España permitió que los datos personales, publicados por terceros, sean borrados de los índices de los buscadores cuando la información sea irrelevante, aunque esta no sea perjudicial e incluso a pesar de haber sido recogida de forma lícita. En el caso Gloria *v.* El Tiempo, la Corte Constitucional Colombiana, en cambio, llegó a una solución diferente aunque los hechos eran similares a los de Google España. Aquí se argumentará por la importancia de reconocer el derecho al olvido siempre que: i) la difusión de los datos personales sea perjudicial para el individuo, y ii) siempre que la información (o el sujeto) de los datos personales no sean de interés público. La inexistencia de este derecho puede congelar expresiones democráticas de los usuarios de internet y contribuye a la asimetría de poder que existe entre los individuos y los procesadores de información.

Palabras clave: derecho al olvido, libertad de expresión, privacidad, datos personales, Google, El Tiempo.

ABSTRACT

In the Google *v.* Spain case, the European Court of Justice allowed the deletion of personal data, published by third parties, from Internet search engines. Accordingly, personal data can be erased whenever the information is irrelevant –even if it is not harmful, although it is true and even if it has been legally obtained. In contrast, in the case Gloria *v.* El Tiempo, the Colombian Constitutional Court reached a different solution although the facts where similar to the Google Spain case. I will argue for the importance of recognizing the right to be forgotten whenever (i) the dissemination of personal data is harmful to the individual and (ii) as long as the the personal data is not of public interest. The non-existence of this right can chill democratic expressions on the Internet, and it might contribute to the

* Candidata a doctora, Universidad de los Andes, Bogotá.

asymmetry of power that exists between individuals and controllers or processors of information.

KEYWORDS: the right to be forgotten, freedom of expression, privacy, personal data, Google, El Tiempo.

FORO

Ireneo Funes, cuenta Borges, lo recordaba todo. Después de un accidente, Ireneo quedó tullido, pero en cambio adquirió una memoria ilimitada, infalible. Todo lo visto, pensado o sentido no podía borrársele. Decía: "más recuerdos tengo yo solo que los que habrán tenido todos los hombres desde que el mundo es mundo".[1] Funes murió a los 21 años de una congestión pulmonar, congestión que alude a los incesantes y minuciosos recuerdos que terminan por inundar y sofocar su mente.[2] En "Fragmentos sobre Joyce", Borges explica la naturaleza de Funes como un "precursor de los superhombres, un *Zarathustra* suburbano y parcial".[3] La monstruosa memoria de Ireneo lo ubica por fuera del reino humano, un espacio en donde habitamos todos aquellos que, a diferencia de Ireneo, tenemos la capacidad de olvidar. En ese mismo reino también está el internet que, como Ireneo, almacena ilimitadamente datos y carece de la capacidad humana de crear ideas generales y de pensar, porque para abstraer y categorizar es preciso suprimir las particularidades, ejercer la memoria afectada por el olvido y crear.

En 2012, la Corte Europea de Justicia reconoció en el caso Google *v.* España el derecho al olvido. Este derecho permite solicitar a los motores de búsqueda en internet la eliminación de información personal que haya sido publicada por terceros y que se encuentre en esos buscadores. Los motores de búsqueda, como Google, deben entonces proceder a desindexar de sus bases de datos la información que hayan capturado de las páginas de internet, como periódicos, blogs o revistas.

La inclusión de este nuevo derecho no ha pasado inadvertida. Un ring con defensores y detractores se ha venido construyendo a partir de este caso, y en el marco de discusiones sobre el tratamiento de datos personales en la era digital. A un lado del cuadrilátero, sus defensores consideran que el olvido –como característica humana–

1. Jorge Luis Borges, "Funes el memorioso", en *Ficciones* (Buenos Aires: Emecé, 1965), 22.
2. James Ramsey, "Sinécdoque y parasitismo literario en Borges y Joyce", *Literatura: teoría, historia, crítica*, No. 12 (2010): 106.
3. Ibíd., 106.

debe también trasladarse al mundo cibernético pues un derecho de esa naturaleza busca proteger el derecho a la privacidad, el honor y el control de los individuos sobre sus datos personales. Al otro lado, sus detractores consideran que la memoria infalible de internet protege y promueve derechos como la libertad de expresión, la historia o la memoria colectiva.[4]

Este artículo se alineará con la primera posición pero matizará el alcance de este derecho respecto de la ruta que la Corte Europea de Justicia, en el caso Google, trazó para su desarrollo. La Corte permite que los datos personales publicados por terceros sean borrados de los índices de los buscadores no solo cuando aquella información sea perjudicial para el sujeto de esos datos, sino además cuando la información sea irrelevante –aunque esta no sea perjudicial e incluso a pesar de haber sido recogida de forma lícita–. En cambio, aquí se defenderá la importancia de contar con un derecho de esa naturaleza siempre que: i) la difusión de los datos personales sea perjudicial para el individuo, ya sea en su privacidad, libertad o en la posibilidad de controlar sus propios datos personales; y ii) siempre que la información (o el sujeto) de los datos personales no sean de interés público. El ejercicio de este derecho, dentro de esos parámetros, afectaría de manera mínima a la libertad de expresión. Si la protección a la libertad de expresión se justifica en virtud de su función como medio para la formación de la opinión pública, y por lo tanto para profundizar y legitimar la democracia, entonces el almacenamiento y difusión de datos personales –que no son de interés público– por parte de los buscadores de internet no serían variables elementales que contribuyan a la formación de la opinión pública.

En la primera parte de este artículo se describirán los hechos que dieron lugar al Caso Google *v.* España. También se esbozarán los hechos del caso Gloria *v.* El Tiempo, sentencia T-277/15 de la Corte Constitucional Colombiana, que con hechos similares llegó a una solución diferente. Enseguida se analizarán y compararán críticamente ambos casos.

---

4. El índice de censura por ejemplo ha denunciado que el caso Google es "como marchar hacia una biblioteca y forzarla a retirar ciertos libros". Sin embargo, este argumento asume que el almacenamiento de los libros no tiene filtro alguno, que no se seleccionan o rechazan libros de acuerdo a los requerimientos de cada universidad. El cofundador de Wikipedia, Jimmy Wales, ha señalado que el derecho a ser olvidado es "profundamente inmoral [porque] la historia es un derecho humano". Información disponible en: Index on Censorship, "Index Blasts EU court ruling on 'right to be forgotten'", en *Index the voice of expression*, 13 de mayo 2014, ‹https://www.indexoncensorship.org/2014/05/index-blasts-eu-court-ruling-right-forgotten/›; Sophie Curtis y Alice Philipson, "Wikipedia founder: EU's Right to be Forgotten is 'deeply immoral' ", en *The Telegraph*, 6 de agosto de 2014. Disponible en ‹http://www.telegraph.co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html›.

En la segunda parte, se recreará el debate en torno al reconocimiento de este derecho, se explicará su pertinencia en el marco de la era digital, y finalmente se sugerirán algunos límites para su adecuada confección.

LOS CASOS PARADIGMÁTICOS

Google *v.* España

En 1997 Mario Costeja incurrió en deudas relacionadas con la Seguridad Social. Para saldarlas sus inmuebles fueron embargados, y para rematarlos el Ministerio de Trabajo y Asuntos Sociales ordenó dar máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores.[5] El periódico *La Vanguardia* procedió a su publicación, y el proceso legal continuó hasta su finalización. Casi dos décadas más tarde, cuando un usuario introducía el nombre de Costeja en el motor de búsqueda de Google obtenía como resultado vínculos hacia dos páginas del periódico *La Vanguardia* en las que figuraba el anuncio de dicha subasta. En el año 2010, Costeja presentó un reclamo ante la Agencia Española de Datos (AEDP) en contra del periódico *La Vanguardia*, Google Inc., y Google España.

El reclamo formulaba dos peticiones: 1. Que se exigiese a *La Vanguardia* eliminar o modificar la publicación de tal manera que no apareciesen sus datos, o que se utilicen las herramientas facilitadas por los motores de búsqueda para proteger dichos datos. En efecto, los editores de internet (periódicos, blogs) pueden utilizar herramientas como "robots.txt",[6] que sirven precisamente para no indexar en los buscadores de internet cierta información que publican en sus páginas. De esta manera, el internauta solo puede acceder a esa información si va directamente a la página de internet, pero ya no a través de los motores de búsqueda. 2. Que se exigiese a Google España o Google Inc. la eliminación u ocultamiento de sus datos personales para que su nombre no esté ligado con los enlaces de *La Vanguardia*. Costeja argumentaba que el embargo había concluido hace años y carecía de relevancia actual.

La AEDP desestimó el reclamo en contra de *La Vanguardia*, pues consideró que la publicación tenía una justificación legal al haber sido ordenada por el Estado para

5. Corte Europea de Justicia, Google *v.* España, 13 de mayo de 2014.
6. Los robots son "arañas" o robots de indexación que funcionan como programas informáticos utilizados para rastrear y realizar un barrido del contenido de páginas web de manera metódica y automatizada. Google almacena temporalmente en servidores cuyo estado de ubicación se desconoce, ya que este dato es secreto por razones competitivas. Ver: ibíd., párrafo 41.

llevar a cabo una subasta. En cambio, aceptó el reclamo en contra de Google al considerar que los motores de búsqueda son responsables del tratamiento de datos personales y, como tales, están sometidos a la normativa en materia de protección de datos, particularmente la Directiva 95/46, que regula el uso y almacenamiento de datos personales en los países de la Unión Europea. En consecuencia, la AEDP ordenó la eliminación de los datos de Costeja de los motores de búsqueda de Google. Google España y Google Inc. apelaron la decisión ante la Audiencia Nacional, la cual a su vez suspendió el procedimiento y pidió una interpretación de la Corte Europea de Justicia acerca de los artículos 2.b y 2.d;[7] y los artículos 12[8] y 14,[9] de la Directiva 95/46.

---

7. Art. 2. Definiciones.- A efectos de la presente Directiva, se entenderá por: b) "tratamiento de datos personales" ("tratamiento"): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción; [...] d) "responsable del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario.
8. Art. 12. Derecho de acceso.- Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del art. 15; b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos; c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.
9. Art. 14. Derecho de oposición del interesado.- Los Estados miembros reconocerán al interesado el derecho a:

   a) oponerse, al menos en los casos contemplados en las letras e) y f) del art. 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos; b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de estos a

Las respuestas de la Corte, relevantes para este estudio, fueron dos:

1. La Corte determinó que las actividades que realizan los motores de búsqueda –localizar información, indexar y almacenar– pueden efectivamente entenderse como "tratamiento de datos personales", y por lo tanto los motores son "responsables" por dicho tratamiento, de acuerdo a los artículos 2.b y 2.d de la Directiva 95/46. Con esta premisa, la Corte Europea estableció que se puede pedir directamente a Google la retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información, y aun cuando la información que ahí repose sea legal.
2. La Corte estableció que los derechos que otorga la Directiva, en sus artículos 12 y 14 a solicitar la supresión y bloqueo de datos personales, así como la oposición para el tratamiento de esos datos, incluye el derecho a que el interesado pueda impedir a los buscadores la indexación de la información referida a su persona –publicada en páginas web de terceros– argumentando que no desea que esa información sea conocida por los internautas, ya sea porque considere que puede perjudicarle o cuando simplemente desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros.

El caso Gloria *v.* El Tiempo: sentencia T-277/15 de la Corte Constitucional Colombiana

Hace quince años, Gloria trabajaba como vendedora en una agencia de viajes. Ella vendió boletos aéreos a un comprador, quien resultó estar relacionado con una red de trata de personas. Debido a esas transacciones, la Fiscalía vinculó a Gloria en un proceso penal, del cual resultó exonerada debido a la prescripción de la acción penal. La existencia de esta red y la captura de Gloria fueron publicados por el periódico *El Tiempo*, noticia que hasta la fecha de la interposición del recurso de hábeas data por parte de la actora todavía seguía disponible en internet. La noticia no hacía alusión a la exoneración de Gloria, quien argumenta que dicha información le "somete a tener un registro negativo ante la sociedad, lo que a su vez le genera traumatismos a ella y su familia para desarrollar actividades en su vida diaria, como la realización de trámites

---

efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización. Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b).

ante entidades financieras o la búsqueda de empleo".[10] Alegaba que se vulneraba sus derechos a la honra, el buen nombre y la intimidad pues la publicación no informaba que no fue vencida en juicio debido a la prescripción de la acción.

Gloria solicitó la eliminación de esa noticia, pero *El Tiempo* señaló que la eliminación no tenía lugar toda vez que la noticia era veraz e imparcial. La actora entonces solicitó, mediante tutela, que se ordene a *El Tiempo* bajar y borrar de todos los buscadores cualquier información negativa relacionada con la supuesta comisión del delito de trata de personas. El caso llegó al conocimiento de la Corte Constitucional; se enfatizará en las respuestas que la Corte dio respecto de: quién es el responsable de la información personal; si la publicación e indexación a Google vulnera los derechos fundamentales de Gloria; y, de ser el caso, cuál sería el remedio.

La Corte Constitucional se pronunció primero acerca de si los motores de búsqueda pueden ser responsables del tratamiento de datos personales. Así, contestó negativamente, al interpretar un informe de la Relatoría Especial sobre Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), ubicó a los motores de búsqueda como *meros transmisores* que ofrecen acceso y búsqueda de información, sin ser responsables de los contenidos generados por terceros. Con esto, el análisis se centró en la responsabilidad de El Tiempo y el alcance del derecho al hábeas data. El razonamiento de la Corte giró en torno a la veracidad, precisión o falsedad de la información a fin de permitir su eliminación o su rectificación. Estimó que en el caso, hay una coalición de derechos fundamentales: por un lado los derechos a la libertad de expresión de *El Tiempo* y a la información de toda la sociedad, y, por el otro, los derechos a la honra y al buen nombre de Gloria.[11]

La Corte Constitucional colombiana finalmente señaló que la noticia es incompleta, y que la falta de actualización, más el tiempo por el cual la información ha estado disponible, generó que el hecho público no estuviera protegido por el derecho a la información, consecuentemente vulnerando los derechos a la honra y al buen nombre de Gloria. La Corte Constitucional estableció que si bien la rectificación de la información sería el remedio correspondiente, no es suficiente pues el largo tiempo por el cual la información estuvo disponible sometió a Gloria a un duro señalamiento público que pudo haber vulnerado otras garantías, como el derecho al trabajo. El remedio entonces consistió en ordenar al medio de comunicación –y no a los motores de búsqueda– hacer uso de las herramientas técnicas como "robots.txt" para evitar que los buscadores accedan a la noticia que narra la captura y el procesamiento de la accionante.

---

10. Corte Constitucional Colombiana, Sentencia T-277/15, 12 de mayo de 2015.
11. Ibíd, párrafo 9.1.

Comparación y comentario

La responsabilidad de los motores de búsqueda

Los buscadores, como intermediarios de la información, no producen datos, sino que su actividad consiste en localizar información publicada por terceros en internet, indexarla automáticamente, almacenarla temporalmente y difundirla o ponerla a disposición de la usurarios de internet según un orden de preferencia determinado. La Corte Europea señaló que, cuando esas actividades incluyen datos personales, existe un *tratamiento* de datos personales por parte del buscador. El paso importante que dio la Corte Europea de Justicia fue calificar como *responsable* de ese tratamiento a Google.[12] La Corte Colombiana, en cambio, enmarcó la responsabilidad solo dentro de actividades que tienen que ver con la generación del *contenido* de la información y no por su localización y difusión. Para la Corte Colombiana, las actividades de difusión y transmisión colocan a Google como mero transmisor de datos, que, no obstante, de acuerdo con la Corte, le permiten a Google jugar un papel indispensable y protagónico en garantizar la libertad de expresión en internet. Resulta extraño, sin embargo, que frente a este gran papel que juegan los buscadores como Google, la Corte Constitucional colombiana no le asigne ninguna responsabilidad respecto del manejo de los datos personales. La Corte presupone que Google no los maneja debido a que solo cumple con el deber de transmitirlos. En consecuencia, el papel de estos buscadores fue valorado por ambas Cortes pero la contrapartida de sus responsabilidades fue concebida de manera distinta.

La Corte Europea abordó el papel decisivo de Google en la difusión global de datos y la facilitación al acceso por parte de los usuarios que, de no contar con este buscador, no podrían conocer dicha información. Como contrapartida, enfatizó que existen riesgos asociados con la información de datos personales que se difunden, especialmente debido a que la actividad de Google equivale a acceder a una lista sobre diferentes aspectos de la vida de una persona. Este acceso es lo que permite al internauta tener una idea más o menos estructurada de quién es el individuo.[13] En esa medida, para la Corte Europea, las responsabilidades de Google y de los editores de

12. De acuerdo a la Directiva 95/46, el responsable del tratamiento de datos personales es quien "solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales". Los medios vendrían a ser los instrumentos digitales que utilizan para localizar, almacenar y difundir los datos personales; y el fin de los datos: el esparcimiento de la información con fines, particularmente económicos.
13. Corte Europea de Justicia, Google *v.* España, párrafo 33.

internet son diferentes. Mientras que los editores de las páginas de internet pueden mostrar una noticia de esa persona, no pueden evitar por otro lado el *esparcimiento* de esa información y su subsecuente reinterpretación por parte de otros editores. Asimismo, Google, a diferencia de los editores, tiene como fin arrojar todos los resultados posibles sobre una misma búsqueda. Este efecto multiplicador de la información, propio de los motores de búsqueda, fue reconocida por la Corte colombiana como una virtud de internet, como una garantía de la libertad de expresión y la democracia, sin embargo, no midió los riesgos inherentes a esa actividad, ni diferenció entre los daños que puede generar *la difusión* multiplicada de la información de datos personales y *el contenido* de las páginas de internet.

Por eso el remedio de las Cortes es diferente. La Corte Europea consideró que no es suficiente con que sea el propio editor de internet quien directamente desindexe su página de los buscadores de Google. Este fue, en cambio, el remedio que adoptó la Corte colombiana al reconocer únicamente la responsabilidad, en virtud del contenido, por parte de los editores de internet. Para la Corte Europea de Justicia, Google puede afectar de manera *adicional* y significativa los derechos fundamentales de respeto a la vida privada y a la protección de datos personales, no por el contenido de la información, sino por el efecto multiplicador de la difusión. En cambio, para la Corte constitucional colombiana, permitir que sea Google quien desindexe directamente las páginas de internet sería una forma de "censura previa",[14] prohibida por los principios de libertad de expresión, aplicables también a internet.

La Corte Constitucional señaló dos motivos por los cuales el remedio europeo no es factible. Primero, porque la desindexación de las bases de datos de Google también permite que la noticia sea accesible si se conoce la dirección exacta del sitio web, lo cual expondría de todas formas los derechos al buen nombre de la actora.[15] Aunque esto es cierto, el remedio que adoptó la Corte colombiana sigue permitiendo este acceso, pues no está ordenando la eliminación de la información de esa página. No obstante, al permitir que el periódico sea el que desindexe, no evita la propagación de otras páginas de internet que contengan esa misma información, con lo cual ahonda la violación a esos derechos. Segundo, permitir que sean los buscadores quienes eliminen la información equivaldría, según la Corte colombiana, a violar la libertad de expresión y el principio de neutralidad que garantizan el acceso a internet en condiciones de igualdad para todas las personas. Aunque esta consideración es acertada, la Corte no analizó: por un lado, en qué medida la eliminación de esta información, a partir de la naturaleza personal de esos datos y la función de Gloria en la vida pública,

14. Corte Constitucional Colombiana, Sentencia T-277/15, párrafo 9.8.2.
15. Ibíd., párrafo 9.8.2.

pueden aumentar o disminuir el espacio democrático en internet; y, por otro lado, cuál es el beneficio de los internautas de acceder a esa información frente a la violación de los derechos de Gloria por la difusión masiva de esos datos. Parecería que tratándose de este tipo de datos personales, la violación a los principios que la Corte Constitucional colombiana intenta salvaguardar es mínima en relación con la violación adicional que Gloria sufre en los derechos mencionados. Adicionalmente, la Corte indicó que la posibilidad de que sean los buscadores quienes eliminen la información implica la existencia de controles previos o de censura, aún a pesar de que las solicitudes en el caso de Gloria y en el caso de Google España fueron posteriores a la publicación de la noticia.

El alcance del derecho a la eliminación de la información

El control de los datos personales puede incluir: la actualización, la rectificación o la eliminación de los datos. Esto a su vez depende del tipo de datos que se trate, del daño que cause, de su licitud (o veracidad) y de su relevancia. La respuesta de ambas Cortes también difirió en este punto. La Corte Europea, presuponiendo la responsabilidad de los motores de búsqueda, dio aquí el paso decisivo para la configuración del derecho al olvido: el usuario puede pedir la eliminación de su información personal publicada por terceros cuando le resulte perjudicial o cuando simplemente quiera que la información ya no se difunda, pues es irrelevante; es decir, cuando quiera que la información sea olvidada tras un período de tiempo después del cual aquella no es útil, incluso si la información es verdadera y no es perjudicial para el usuario. Para la Corte colombiana, en cambio, la posibilidad de controlar los datos personales solo existe en el caso de que la información sea inexacta, incompleta o falsa. Lo que quiere decir que, si la información es verdadera, el individuo no tendría el derecho a la eliminación de sus datos.

La Directiva europea 46/95, cuyo objeto es la protección de los datos personales, establece que los responsables deben garantizar que el tratamiento de los datos sea: a) leal; b) recogidos con fines determinados; c) explícitos y legítimos, adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben; d) exactos y, cuando sea necesario, actualizados; y f) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos.[16] Para el estándar colombiano la eliminación de

16. Parlamento Europeo, Consejo de la Unión Europea, *Directiva 46/95/CE*, 24 de octubre de 1995, art. 6.

los datos solo procedería en el caso de la letra d); es decir, cuando no sean exactos o cuando la información sea falsa y genere una violación a los derechos fundamentales. En el caso europeo, en cambio, la Corte de Justicia configuró el derecho al olvido enfatizando que el derecho de eliminación de los datos no presupone que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado[17] y se puede solicitar cuando el tratamiento de los datos no haya respetado cualquiera de los literales indicados. En otras palabras, el usuario puede pedir la eliminación de la información si resulta irrelevante con el paso del tiempo, inclusive si no hay perjuicio alguno.

En esta parte, el razonamiento de la Corte es poco detallado especialmente porque, en el caso en cuestión, Costeja solicita la eliminación en virtud de la violación a sus derechos a la privacidad y al honor. La Corte Europea da un paso más y reconoce la posibilidad de eliminar información personal a la luz de más presupuestos y sin que medie daño alguno. El derecho al olvido, sin embargo, tampoco es ilimitado. El tratamiento de esos datos no solo debe violar los requisitos establecidos en los literales que anteceden (licitud, relevancia...), sino que además se debe demostrar que no hay una razón legítima que justifique su tratamiento. La Corte Europea no encontró una razón suficiente para no eliminar la información de los buscadores. Por un lado, la publicación ya cumplió con el interés para el cual fue concebido. Por otro lado, aunque reconoció que algunos internautas podrían beneficiarse de esa información, explicó que la naturaleza de los datos y el papel que desempeña en la vida pública el señor Costeja no justifican la violación a la privacidad y la protección de los datos personales.

El razonamiento de la Corte colombiana en este punto es similar pero se restringe al daño que ocasiona el contenido de la noticia, y no a su difusión. Para justificar su decisión la Corte hace alusión a la naturaleza del crimen y las consecuencias sociales. Señala que:

> La conducta por la cual se investigó y procesó al accionante, la trata de personas, es un delito que, a diferencia de otros, recibe un rechazo especialmente grave por parte de la comunidad, por lo que para una persona el simple hecho de haber estado relacionado con una investigación penal por este delito puede tener serias repercusiones en sus relaciones personales, familiares y laborales.[18]

Por ello, ordena que sea el periódico el que evite que los buscadores de internet accedan a la noticia que narra la captura y procesamiento de la accionante por el delito de trata de personas, pues a su entender es la solución que mejor equilibra los

17. Corte Europea de Justicia, Google *v.* España, párrafo 96.
18. Corte Constitucional Colombiana, Sentencia T-277/15, párrafo 9.8.3.

principios constitucionales en tensión. Por lo tanto, la Corte colombiana permite que los periódicos no indexen información personal a los buscadores siempre que esa información sea inexacta y que vulnere los derechos fundamentales de las personas. La Corte Europea, en cambio, permite que los buscadores eliminen cualquier información asociada con el nombre del individuo cuando esa información no solo sea inexacta, sino también irrelevante y aun cuando no haya vulneración a los derechos fundamentales. Es precisamente, la inexistencia del daño lo que parecería desconfigurar el balance entre los derechos a la privacidad y la libertad de expresión.

RECREANDO EL ALCANCE Y LA NECESIDAD DEL DERECHO AL OLVIDO EN EL CONTEXTO DE LA LIBERTAD DE EXPRESIÓN Y LA PRIVACIDAD

Antes que el derecho al olvido viera la luz en la sentencia de la Corte Europea, ya tenía raíces intelectuales en Francia, donde se había reconocido un *droit à l'oubli* a favor de los criminales convictos que ya habían servido su condena. Dicho derecho les permitía objetar publicaciones de los hechos sobre su pena y encarcelamiento. Los mismos presupuestos, sin embargo, son tratados de manera radicalmente opuesta en Estados Unidos, donde la publicación del pasado criminal está protegida por la Primera Enmienda.[19] El reconocimiento de este derecho a nivel europeo, y aplicado al espacio cibernético, ha provocado un debate entre "preservasionistas" y "suprimistas".[20] Los primeros creen que el internet ofrece la más verdadera y comprehensiva historia de la humanidad que jamás haya sido recolectada, y sienten un deber hacia las futuras generaciones de preservar de manera intocada los legados digitales; asimismo, consideran que borrar la información de internet es la mayor amenaza a la libertad de expresión cuando la información ha sido recogida de manera legal y cuando es verdadera, aunque resulte perjudicial. Los segundos, en cambio, argumentan que internet debe aprender a olvidar para poder preservar valores sociales que son vitales; además, señalan que la cultura humana no puede manejar una memoria absoluta sin amenazar a la dignidad y a la privacidad de las personas y sin crear un sociedad abierta, pero opresiva en el espacio cibernético.[21]

---

19. Jeffrey Rosen, "The Right to be Forgotten", *Stanford Law Review* (2012). Disponible en ‹https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/›.
20. Meg Leta Ambrose, Nicole Friess y Jill Van Matre, "Seeking Digital Redemption: The future of forgiveness in the Internet Age", *Santa Clara & High Tech. L.J.*, vol. 29 (2012): 112.
21. Ibíd., 112.

Ahora bien, en internet ya se elimina información de todo tipo. Algunos estudios en la persistencia de la información en internet han demostrado que una cantidad significativa de datos desaparece cada día.[22] Más interesante para los propósitos de este artículo es la arquitectura del internet y el alcance de este derecho. Peter Fleischer ha identificado tres escenarios de eliminación de los datos personales que varían según la intensidad a la libertad de expresión. El primero, en donde el dueño de la información sube por sí mismo sus datos –como fotos a Facebook– y luego puede eliminarlos; un servicio que casi todas las plataformas de este tipo ya proveen y que demuestra que un internet sin agujeros de información no es posible. El segundo escenario, en donde el individuo sube información personal, y luego es copiada por otra persona en otro sitio; aquí se presentan algunas dificultades respecto de quién es el dueño de la información y el hecho de que la eliminación dependería de la voluntad de terceros.[23] Finalmente, el escenario más polémico, en donde otros publican información personal de un individuo y este solicita a los intermediarios de internet que eliminen dicha información.[24] Es aquí, frente a la contemplación de Google y otros buscadores, que actuarían como jueces de lo que se elimina o no, en donde los críticos del derecho al olvido trazan la línea. El argumento es que los buscadores no producen el contenido, sino que lo difunden. Según los críticos, el rol que juega Google en mantener la neutralidad de la web se vería socavado al entregarles un poder de censura. Sin embargo, el rol de los buscadores no es necesariamente neutral ni tampoco permite un flujo absoluto y libre de información. Los buscadores poseen un cierto control de la información: arrojan resultados después de filtrar la información a partir de un orden de preferencias, generalmente, comerciales. Además, Google y otros buscadores ya tienen mecanismos para remover contenido ilegal o inaceptable, algunos países utilizan la propiedad intelectual para eliminar información dañosa, como el caso de la pornografía infantil o la venganza pornográfica.[25]

Borrar la información personal de internet ha sido criticado también por chocar contra el acceso a datos de interés público.[26] Qué tipo de información es de inte-

---

22. Ravi Antani, "The resistance of memory: Could the European Union's right to be forgotten exist in the United States?", *Berkeley Technological Law Journal*, No. 30 (2015): 1206.
23. Por ejemplo el famoso caso de Da Cunha en Argentina. Ver: Edward Carter, "Argentina's Right to be Forgotten", *Emory International Law Review*, No. 27 (2016): 23-39.
24. Peter Fleicher, "Foggy Thinking about right to oblivion", *Peter Fleicher: Privacy...?* Disponible en ‹http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html›.
25. Peter Fleicher, "The right to be forgotten or how to edit your history", *Peter Fleicher: Privacy...?* Disponible en ‹http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html›.
26. James Balle, "EU's right to be forgotten: Guardian articles have been hidden by Google", *The Guar-*

rés público es un estándar que se debe desarrollar jurisprudencialmente y que debe atender a preguntas como: ¿La eliminación de la información afecta un interés de la comunidad o solo un interés individual? ¿Es necesaria para la formación de la opinión pública? ¿Su conocimiento por parte de las autoridades puede mejorar la situación de la comunidad?

El derecho al olvido debe pues, reservarse para cuestiones que afectan a la privacidad individual y no inciden en la generación y el flujo de información pública. Los datos de figuras públicas o los crímenes de naturaleza sexual tendrían una presunción fuerte de ser conocidos por parte de toda la comunidad. Por información personal uno podría pensar en fotos embarazosas, artículos de periódico, comentarios que capturan posiciones políticas polémicas o poco populares. La posibilidad de que esa información permanezca perennemente en la web, de que los individuos no puedan escaparse de su pasado, tiene dos efectos importantes.

Primero, afecta a la autonomía y a la libertad personal. Si hay pocas regulaciones en internet, si no es posible eliminar de los buscadores datos personales que no contribuyen al debate púbico, entonces es probable que los individuos tengan miedo a expresarse libremente porque su información y sus acciones estarían a disposición de todos. En otras palabras, habría un congelamiento de las expresiones democráticas. Por supuesto, si hay muchas regulaciones todas las acciones de un individuo se excluirían del reino de lo público y eso afectaría al libre flujo de ideas; es lo que Post denomina "la paradoja del discurso público".[27] Encontrar el balance dependerá, al fin, del contexto y de la valoración que cada cultura constitucional asigne a uno y otro principio.

No obstante, lo que está en juego con el reconocimiento del derecho al olvido no es el contenido político de la información, sino la *difusión de información personal* de gente común y corriente. Las deudas públicas de Costeja, por ejemplo, son una información vergonzosa que, tras más de una década, dice poco acerca de su carácter. Como señala Posner, "la privacidad nos permite experimentar, cometer errores y comenzar de nuevo si lo arruinamos. Nos permite reinventarnos [tener] segundas oportunidades...". [28] En efecto, la posibilidad de ser condenados por los errores del pasado puede traer consecuencias dañinas para el proyecto de vida de un individuo.

---

dian, 2 de julio de 2014. Disponible en ‹https://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google›.

27. Robert Post, "The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and Hustler Magazine *v.* Falwell", *Harvard Law Review*, No. 103 (1990): 640.
28. Eric Posner, "We all have the right to be forgotten", *Slate*, 14 de mayo de 2014. Disponible en ‹http://

Segundo, evitar que internet olvide afecta el control que los individuos puedan tener sobre sus datos personales, con lo cual también se socava la posibilidad de tomar decisiones autónomamente respecto de cuestiones vitales. En efecto, controlar los datos personales no solo es importante en el contexto de la protección a la privacidad, sino también en un contexto de asimetría de poder entre los individuos y los procesadores de información. Orla ha señalado que la asimetría de poder genera dificultades a los individuos a la hora de establecer la posibilidad de que la entrega de su información pueda ser potencialmente dañosa, o el hecho de que cuando eso ocurre es difícil hacer responsables a quienes procesaron la información.[29] Entregar a los individuos el control sobre sus datos parece ser una forma de equilibrar esta relación de poder.

Por último, el reconocimiento del derecho al olvido debe presuponer la existencia de un daño a la privacidad, al control de los datos, o a la libertad personal. Google *v.* España diluye este presupuesto. Al hacerlo, la Corte Europea se despoja del elemento que hace posible la reconciliación del derecho al olvido con el discurso público necesario para la legitimación democrática.[30] En consecuencia, si la información no causa ningún daño, eliminar información de la web provocaría una violación injustificada a la libertad de expresión. El derecho al olvido profundiza la protección a la privacidad, pues permite que la información personal sea menos pública y, por tanto, disminuye los efectos negativos en la vida de los individuos. Sin embargo, el ejercicio de este derecho debe ser confeccionado de manera correcta a fin de maximizar el potencial expresivo del internet y aquietar la ansiedad relacionada a una existencia totalmente expuesta o absolutamente inhibida en la red.[31]

CONCLUSIÓN

Las experiencias de Google España y de *El Tiempo* ayudan a comprender que la difusión y almacenamiento de los datos personales en internet debe ser considerado y cautelosamente regulado. Mientras que la difusión es fundamental para profundizar la democracia, como argumenta la Corte Constitucional colombiana, la difusión ili-

---

www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html›.

29. Lynskey Orla, "Deconstructing Data Protection: The 'Added-Value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, No. 63 (2014): 522.
30. Robert Post, "News on the Web: Google Spain, the Right to Be Forgotten, and Personal Data". Ponencia presentada en el Faculty Workshop, New Haven, 17 de octubre de 2016, 19.
31. Ambrose, Friess y Van Matre, "Seeking Digital Redemption: The future of forgiveness in the Internet Age", 113.

mitada de los datos personales puede conllevar también a la autocensura, al congelar expresiones democráticas de individuos temerosos de que sus opiniones o actividades no puedan ser nunca olvidadas, siendo por lo tanto más cuidadosos a la hora de expresar libremente lo que piensan, absteniéndose de expresarlo del todo. En esta medida, tal como argumenta la Corte Europea, cuando la información de un individuo permanece ilimitadamente en los buscadores, puede incidir negativamente en las posibilidades de su desarrollo vital: en encontrar un trabajo, acceder a financiamiento, tener capital social, entre otras.

Sin embargo, el alcance que dio la Corte Europea al derecho al olvido es muy vasto y podría afectar desproporcionadamente a la libertad de expresión pues elimina la posibilidad de que para remover la información personal exista de por medio un daño al individuo. No obstante, el libre flujo de ideas y de información presupone espacios deliberativos, en donde la información no es dañina para los individuos o –si lo fuera– sea necesaria en función de su importancia pública. Por lo tanto, eliminar el daño como requisito para la eliminación de la información perjudica la arquitectura misma de la libertad de expresión en sociedades democráticas.

Finalmente, el reconocimiento del derecho al olvido es un imperativo porque aunque el internet sea un espacio democrático, en las sociedades actuales la relación entre los procesadores y controladores de datos personales y los dueños de esos datos no lo es. La asimetría de poder entre ambos actores podría impedir que personas ordinarias, usuarias de internet, no puedan pedir la remoción de sus datos. El derecho al olvido ayudaría a restablecer un balance gracias a que le entrega al usuario un mayor control sobre sus datos personales.

BIBLIOGRAFÍA

Ambrose, Meg Leta, Nicole Friess y Jill Van Matre. "Seeking Digital Redemption: The future of forgiveness in the Internet Age". *Santa Clara & High Tech. L.J.*, vol. 29 (2012).

Antani, Ravi. "The resistance of memory: Could the European Union's right to be forgotten exist in the United States?". *Berkeley Technological Law Journal*, No. 30 (2015).

Balle, James. "EU's right to be forgotten: Guardian articles have been hidden by Google". *The Guardian*. 2 de julio de 2014. Disponible en ‹https://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google›.

Borges, Jorge Luis. "Funes el memorioso". En *Ficciones*. Buenos Aires: Emecé, 1965.

Carter, Edward. "Argentina's Right to be Forgotten". *Emory International Law Review*, No. 27 (2016).

Curtis, Sophie, y Alice Philipson. "Wikipedia founder: EU's Right to be Forgotten is 'deeply immoral' ". En *The Telegraph*, 6 de agosto de 2014. Disponible en ‹http://www.telegraph.

co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html›.

Fleicher, Peter. "Foggy Thinking about right to oblivion". *Peter Fleicher: Privacy...?* Disponible en ‹http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html›.

---. "The right to be forgotten or how to edit your history". *Peter Fleicher: Privacy...?* Disponible en ‹http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html›.

Index on Censorship. "Index Blasts EU court ruling on 'right to be forgotten' ". En *Index the voice of expression*. 13 de mayo de 2014. Disponible en ‹https://www.indexoncensorship.org/2014/05/index-blasts-eu-court-ruling-right-forgotten/›.

Orla, Lynskey. "Deconstructing Data Protection: The 'Added-Value' of a right to data protection in the EU legal order". *International and Comparative Law Quarterly*, No. 63 (2014).

Posner, Eric. "We all have the right to be forgotten". *Slate*, 14 de mayo de 2014. Disponible en ‹http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html›.

Post, Robert. "News on the Web: Google Spain, the Right to Be Forgotten, and Personal Data". Ponencia presentada en el Faculty Workshop, New Haven, 17 de octubre de 2016.

---. "The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and Hustler Magazine *v.* Falwell". *Harvard Law Review*, No. 103 (1990).

Ramsey, James. "Sinécdoque y parasitismo literario en Borges y Joyce". *Literatura: teoría, historia, crítica*, No. 12 (2010).

Rosen, Jeffrey. "The Right to be Forgotten". *Stanford Law Review* (2012). Disponible en ‹https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/›.

Fecha de recepción: 24 febrero de 2017
Fecha de aprobación: 1 de mayo de 2017

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

Colaboradores

Alexander Cuenca Espinosa: ecuatoriano, abogado, Pontificia Universidad Católica del Ecuador; especialista en Derecho Penal y Delitos Informáticos, Instituto de Altos Estudios Universitarios, Barcelona; doctor en Ciencias Jurídicas, Universidad Católica Argentina; becario de la especialización en Derecho Notarial y Registral del Instituto de Altos Estudios Nacionales del Ecuador. Docente de posgrado de la Maestría en Seguridad y Riesgo de la Universidad de la Fuerzas Armadas (ESPE). Articulista y consultor internacional en áreas de inteligencia cibernética, crimen organizado y ciberdelitos. *alexandercuencaespinosa@gmail.com*

Luis Enríquez Álvarez: ecuatoriano, abogado, Universidad Internacional SEK; máster en Derecho, mención Derecho Internacional Económico, Universidad Andina Simón Bolívar, Sede Ecuador; máster en Derecho de tecnologías de la información, Leibniz Universität Hannover. Certificaciones en: Certified Ethical Hacker, EC-Council Certified Security Analyst, Computer Hacking Forensics Investigator (EC-Council), HD Data Recovery Expert (AceLabs). Consultor de seguridad informática, y perito en informática forense. *luis.enriquez@owasp.org*

Gabriela Espinoza Plúa: ecuatoriana, abogada, Universidad San Francisco de Quito; máster en Derecho, mención Derecho Constitucional, Universidad Andina Simón Bolívar, Sede Ecuador; candidata a doctora, Universidad de los Andes, Bogotá. Investigadora asociada de la Universidad de Yale. Autora de varias publicaciones. *marjorie.espinozaplua@yale.edu*

Valentin Gibello, francés, máster en Derecho y doctorando en Derecho público, Université Lille 2 Droit et Santé. Miembro del equipo "Derecho del ciberespacio" del CERAPS, Universidad de Lille 2. Especializado en Derecho de protección de datos personales. *valentin.gibello@univ-lille2.fr*

Marcel Moritz, francés, doctor en Derecho, Université d'Aix-en-Provence. Profesor senior de Derecho público, y director del Máster en Derecho del ciberespacio, Universidad de Lille. Autor de varias publicaciones referentes a la materia. *marcel.moritz@univ-lille2.fr*

Lorena Naranjo Godoy: ecuatoriana, abogada, Pontificia Universidad Católica del Ecuador; magíster, y candidata a doctora en Derecho de las Nuevas Tecnologías, Universidad Pablo de Olavide. Docente a tiempo completo y directora de la Escuela de Derecho de la Universidad de las Américas. Consultora en temas relacionados a Derecho Informático y Derecho Civil. Autora de varias publicaciones. *lorenaranjog@hotmail.com*

Luis Ordóñez Pineda: ecuatoriano, abogado, Universidad Técnica Particular de Loja; máster en Derecho, Universidad Nacional Autónoma de México; candidato a doctor en Ciencias Sociales y Jurídicas por la Universidad de Cádiz-España. Docente-investigador del Departamento de Ciencias Jurídicas de la Universidad Técnica Particular de Loja. Autor de varias publicaciones. *loordonez@utpl.edu.ec*

Claudia Orellana Robalino: ecuatoriana, abogada, Universidad de las Américas; especialista en Derecho Procesal, Universidad Andina Simón Bolívar, Sede Ecuador. Abogada del departamento legal de la Compañía SEDESDE S. A.; asesora legal de la Universidad de Las Américas de Quito. Directora del proyecto "Somos iguales". *claudia.orellana@sedesde.com*

Andrea Villalba Fiallos: ecuatoriana, abogada, Universidad Central del Ecuador; máster en Justicia Criminal, Universidad Carlos III de Madrid. Ex-becaria de la Embajada Francesa de Quito "Programa Asistentes de Idioma". Abogada Patrocinadora del Ministerio de Educación. *andrejvf@hotmail.com*

FORO Revista de Derecho, No. 27,
ISSN 1390-2466 • UASB-E / CEN • Quito, 2017

Normas para colaboradores

1. La revista *FORO* del Área de Derecho de la Universidad Andina Simón Bolívar, Sede Ecuador, publicará únicamente trabajos inéditos, o una versión actualizada de artículos previamente publicados, que ayuden desde una óptica interdisciplinaria a investigar y profundizar las transformaciones del orden jurídico en sus diversas dimensiones y contribuir al proceso de enseñanza de posgrado de derecho en la subregión andina.
2. Los autores, al presentar su artículo a la revista *FORO* declaran que son titulares de su autoría y derecho de publicación, último que ceden a la Universidad Andina Simón Bolívar, Sede Ecuador. El autor que presente el mismo artículo a otra revista, que ya hubiese sido publicado o se fundamente en una versión ya publicada, deberá notificar el particular al editor de la revista.
3. *FORO* edita resultados de artículos de investigación, estudios, experiencias, reseñas y análisis de sentencias.
4. El artículo debe ser remitido a la siguiente dirección electrónica: ‹mariajose.ibarra@uasb.edu.ec›.
5. Los criterios para la presentación de los artículos son los siguientes:
   - Deberán ser escritos en programa de procesador de texto Microsoft Office, Word 7,0 (o inferiores), con tipo de letra Times New Roman, tamaño núm. 12, en una sola cara, interlineado simple. Las páginas estarán numeradas, el texto justificado.
   - Extensión máxima:
     - Artículos: 15 páginas INEN A4 (incluida bibliografía), equivalentes a 8.000 palabras aproximadamente.
     - Análisis de sentencia: 10 páginas INEN A4 (incluida bibliografía), equivalentes a 6.000 palabras aproximadamente.
     - Recensiones: 4 páginas INEN A4 (incluida bibliografía), equivalente a 3.000 palabras.
   - El título del trabajo deberá ser conciso pero informativo, en castellano en primera línea y en inglés. Se aceptan como máximo dos líneas (40 caracteres con espacios).
   - Todo artículo debe ir acompañado del nombre del autor en la parte superior derecha, debajo del título.

- Cada trabajo debe estar acompañado de un resumen de hasta 150 palabras en idioma castellano, donde se describirá de forma concisa el objetivo de la investigación, su contenido y las principales conclusiones.
- Cada trabajo deberá contener un abstract en idioma inglés de 100 a 150 palabras. Para su elaboración no se admite el empleo de traductores automáticos.
- Adicionalmente, se indicarán al menos cinco palabras clave (descriptores) que establezcan los temas centrales del artículo, igualmente en ambos idiomas.
- El autor enviará una reseña de hasta 50 palabras en las que destacará su vinculación académica, publicaciones más importantes y cargo actual. Indicará además su correo electrónico personal.

6. Se debe consignar la dirección y demás datos de ubicación del autor, con el propósito de notificar la recepción de los artículos, así como cualquier decisión del Comité Editorial.
7. Estilo, citas y referencias: se usará el manual de estilo Chicago, a manera de ejemplo:
   - Nombre y apellido del autor, *Título de la obra* (Ciudad: Casa editorial, año), número de página o páginas de donde se tomó la referencia. Por ejemplo: Javier Viciano, *Libre competencia e intervención pública en la economía* (Valencia: Tiran lo Blanch, 1995), 206.
   - En caso de citas posteriores de la misma obra, se señalará únicamente el apellido del autor, título de la obra y número de página, así: Viciano, *Libre competencia e intervención pública en la economía*, 206.
   - Se deberá ser consistente con esta forma de citar a lo largo del texto.
   - Para las citas de revistas o publicaciones periódicas se solicita realizarlas de la siguiente manera: Nombre del autor, título (entre comillas " "), nombre de la Revista (*en cursiva*), tomo o volumen, número del ejemplar (año de publicación): página o páginas citadas. Así: Xavier Gómez, "Los derechos de propiedad intelectual", *Foro: Revista de Derecho*, No. 1 (2003): 85-121.
   - Las referencias bibliográficas deben presentarse al final del artículo bajo el nombre de "Bibliografía" y contendrá los siguientes datos: apellido y nombre del autor. *Título de la obra*, tomo o volumen, número de edición. Ciudad: Casa editorial, año de publicación. No irán numerados y se relacionarán por orden alfabético; por ejemplo: Viciano, Javier. *Libre competencia e intervención pública en la economía*. Valencia: Tirant lo Blanch, 1995.
   - Las citas textuales de hasta cuatro renglones deben escribirse entre comillas y seguido al texto; cuando excedan este número de líneas deben escribirse en párrafo aparte, en un tamaño de letra inferior al resto del texto, con una sangría diferente y con un renglón blanco antes y otro después; si el autor añade algo al texto transcrito deberá ponerlo entre corchetes.

- Tablas, gráficos, cuadros, ilustraciones, etc. deben formar parte del texto del artículo e indicarán claramente el título, número, fuente de procedencia y deberán contener los respaldos en versión original con la descripción de los programas utilizados.
- Cualquier otro aspecto sobre el formato debe resolverse por el autor observando uniformidad y consistencia.

Proceso editorial

FORO acusa recepción de los trabajos enviados por los autores/as y da cuenta periódica del proceso de aceptación/rechazo, así como, en caso de aceptación, del proceso de edición.

1. Los autores podrán remitir manuscritos para su evaluación sin fecha predeterminada, se dará preferencia a los trabajos que se ajusten al eje temático de la convocatoria.
2. En el período máximo de 15 días, a partir de la fecha de recepción, los autores recibirán notificación de recepción, indicando si se acepta preliminarmente el trabajo para su evaluación. Los manuscritos serán evaluados a través del sistema de doble ciego (*peer review*).
3. A la vista de los informes de los evaluadores, se decidirá la aceptación, aceptación con modificaciones, o rechazo de los artículos para su publicación. En caso de aceptación con modificaciones, el autor tendrá un plazo máximo de 15 días para entregar la versión final de su manuscrito.
4. En el caso de juicios dispares, el trabajo será remitido a un tercer evaluador.
5. No existe comunicación directa entre los evaluadores ciegos entre sí, ni entre estos y el autor del trabajo. La comunicación entre los actores está mediada por la coordinadora editorial.
6. Los editores y demás responsables de la revista se reservan el derecho de realizar las correcciones de estilo y modificaciones editoriales que crean necesarias.
7. El plazo de evaluación de trabajos es de 30 días como máximo.
8. Los autores recibirán los informes de evaluación de los revisores, de forma anónima, para que puedan realizar las correcciones o réplicas que correspondan.
9. Una vez editado el número, los autores de artículos recibirán tres ejemplares de la publicación, autores de recensión un ejemplar, y autores de análisis de sentencia un ejemplar.

UNIVERSIDAD ANDINA
SIMÓN BOLÍVAR
Ecuador
25 años

RECTOR
Jaime Breilh Paz y Miño

DIRECTOR DEL ÁREA DE DERECHO
Ramiro Ávila Santamaría

Toledo N22-80 • Apartado postal: 17-12-569 • Quito, Ecuador
Teléfonos: (593 2) 322 8031, 322 8436 • Fax: (593 2) 322 8426
Correo electrónico: ‹ramiro.avila@uasb.edu.ec›, ‹mariajose.ibarra@uasb.edu.ec›
‹www.uasb.edu.ec›

CORPORACIÓN
EDITORA NACIONAL

Roca E9-59 y Tamayo • Apartado postal: 17-12-886 • Quito, Ecuador
Teléfonos: (593 2) 255 4358, 255 4658, 256 6340 • Fax: ext. 12
Correo electrónico: ‹cen@cenlibrosecuador.org›
‹www.cenlibrosecuador.org›

SUSCRIPCIÓN ANUAL (dos números)

Dirigirse a:
CORPORACIÓN EDITORA NACIONAL
Apartado postal: 17-12-886 • Quito, Ecuador
Teléfonos: (593 2) 255 4358, 255 4558 • Fax: ext. 12
‹ventas@cenlibrosecuador.org› • ‹www.cenlibrosecuador.org›

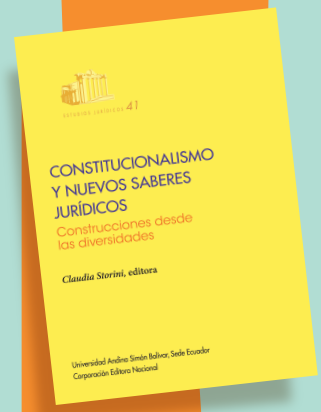
Precio: US $ 33,60

	Flete	Precio suscripción
Ecuador	US $ 6,04	US $ 39,64
América	US $ 59,40	US $ 93,00
Europa	US $ 61,60	US $ 95,20
Resto del mundo	US $ 64,00	US $ 97,60

CANJES

Se acepta canje con otras publicaciones periódicas.

Dirigirse a:
UNIVERSIDAD ANDINA SIMÓN BOLÍVAR, SEDE ECUADOR
Centro de Información
Toledo N22-80 • Apartado postal: 17-12-569 • Quito, Ecuador
Teléfono: (593 2) 322 8094 • Fax: (593 2) 322 8426
Correo electrónico: ‹biblioteca@uasb.edu.ec›



María Elena Jara Vásquez, edit., *Derecho económico contemporáneo*. Quito: Universidad Andina Simón Bolívar, Sede Ecuador / Corporación Editora Nacional, 2017.

Esta obra incorpora reflexiones de prestigiosos académicos de Bolivia, Colombia, Ecuador, España, Italia, México, Perú y Venezuela en torno a los siguientes ejes temáticos: *derechos económicos y sociales:* su alcance y justiciabilidad, al calor de la intervención del Estado en el sistema económico; *regulación y control estatal:* defensa de la competencia, regulación del mercado de valores y evolución del Derecho administrativo en el contexto del cambio de modelos económicos; *economía popular y solidaria:* fundamentos institucionales y conceptuales de este sector y análisis de la dinámica de su funcionamiento; y *derecho de los recursos naturales no renovables:* aspectos jurídicos importantes en torno a los regímenes minero, petrolero y de explotación de gas natural.

Claudia Storini, edit., *Constitucionalismo y nuevos saberes jurídicos: construcciones desde las diversidades*. Quito: Universidad Andina Simón Bolívar, Sede Ecuador / Corporación Editora Nacional, 2017.

Este libro reúne ensayos que buscan contribuir a una nueva teoría del Derecho constitucional pensada desde las diversidades, y elaborar nuevos conceptos o dar nuevos contenidos a los ya existentes, que permitan interpretar la realidad social y hacer frente a la falta de correspondencia entre esta última y la normatividad vigente. Se trata del desarrollo de un pensamiento ligado a la importancia de las interacciones sociales en confrontación con el individualismo como eje de las propuestas tradicionales; de la difusión de un conocimiento colectivo construido en "minga" desde el trabajo social y la participación directa de todos los actores en la búsqueda de soluciones a los problemas de la sociedad.

UNIVERSIDAD ANDINA SIMÓN BOLÍVAR
Ecuador
25 años

CORPORACIÓN EDITORA NACIONAL

9 771390 246002 27