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