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