Panorama de la Normatividad Internacional respecto a la Privacidad de los Datos de los Usuarios de Internet

Víctor Reyes-Macedo, Gina Gallegos-García, Moisés Salinas-Rosales
Instituto Politécnico Nacional - Centro de Investigación en Computación
Av. Juan de Dios Bátiz sn casi esq. Miguel Othón de Mendizábal
Unidad Profesional Adolfo López Mateos Col. Nueva Industrial Vallejo
Alcaldía Gustavo A. Madero C.P 07738, Ciudad de México, México
vreyesm1102@alumno.ipn.mx , ggallegosg@ipn.mx, msalinasr@ipn.mx

***Resumen*—Este trabajo provee al lector de un panorama general sobre la normatividad internacional de la privacidad en el contexto de la cuarta revolución industrial, la era de las comunicaciones y la información. Lo anterior cobra relevancia en un contexto social internacional en donde han surgido controversias respecto a la privacidad de los datos de los usuarios. Para ello, se abordarán tres enfoques: tratados internacionales, legislaciones locales y legislación mexicana. Destaca el hecho de que existen pocos instrumentos legales que permitan a los usuarios de Internet garantizar su derecho a la privacidad, debido a que el contexto de las comunicaciones por este medio recién empieza a ser tomada en cuenta para elaborar dichos instrumentos. De hecho, sólo la Unión Europea y el estado de California en Estados Unidos de América cuentan con un documento que considera específicamente este caso. Los demás, son adaptaciones e interpretaciones de instrumentos de protección de datos ya existentes, como en el caso de México.**

***Index Terms*—Anonimato, derechos humanos, legislación, privacidad , tratados internacionales**

I. Introducción

En el actual contexto global, las tecnologías de la información y comunicación han permitido conectar las diferentes regiones del mundo, haciendo posible el intercambio de información de manera instántanea prácticamente en cualquier lugar. Lo anterior ha generado la apertura de nuevos campos de actividad económica y social para las personas. Por ejemplo, la información generada por los usuarios de plataformas tecnológicas que proveen diferentes servicios, es analizada y usada por las empresas para incrementar sus ganancias mediante diferentes estrategias mercadológicas. Para ello, los usuarios aceptan términos y condiciones de uso que en ocasiones atentan contra su privacidad. De esta forma, otorgan poder a los proveedores de servicios para usar la información generada, con fines comerciales, políticos, y de investigación, entre otros.

Debido a la importancia de la información personal que con diversos motivos se brinda a las empresas u organizaciones a través de Internet, es importante el desarrollo de marcos legales que protejan a los usuarios contra un potencial uso indebido de su información. Por ello, la contribución de este artículo se centra en brindar un panorama sobre la legislación alrededor de este tema en el mundo.

El lector encontrará el artículo organizado de la siguiente forma: en la sección II se habla de conceptos básicos del tema, la sección III aborda los tratados internacionales que retoman la privacidad como un derecho de las personas, la sección IV describe las características de las principales legislaciones en materia de protección de datos que se han desarrollado a nivel regional o nacional. Posteriormente, la sección V retomará el caso de México, y se finaliza con la sección VI que aborda los principales retos y oportunidades para avanzar en este tema.

II. Conceptos Iniciales

En un sentido general, es posible entender el concepto de *privacidad* como la acción de mantener en secreto el contexto en el cual se desarrolla una actividad, a diferencia del *anonimato*, que se centra en mantener secreta la identidad de quien desarrolla una actividad. Por ejemplo, la información bancaria de un tercero es información privada, ya que los datos de los movimientos que realiza no son de acceso público, aún si todos saben a quién pertenece dicha cuenta [1].

El derecho a la privacidad y a la protección de datos es uno de los temas prioritarios en el debate internacional, impulsado en parte por la cantidad de servicios que recolectan y comercian con ellos. A través del tiempo, se han propuesto diversos marcos legales con diferentes objetivos y alcances para proteger los datos de los usuarios de Internet. Sin embargo, no existe un único instrumento legal para abordar problemas sobre seguridad en el ciberespacio, sino que las posibles soluciones surgen de la colaboración entre diferentes disciplinas.

Debido a lo anterior, existen diferentes instrumentos que pueden ser aplicados al entorno digital, como los que se enumeran a continuación. Cabe destacar que a nivel interno, la constitución nacional prevalece sobre otros instrumentos [2].

1. **Tratado:** Se trata de un convenio regido por el derecho internacional público, celebrado por escrito entre Estados o entre Estados y otros sujetos de derecho

internacional, como organizaciones, y bajo el cual cada una de las partes asumen compromisos [3].
2. **Políticas públicas nacionales:** Es una intervención deliberada del Estado, para corregir o modificar una situación reconocida como problema público. También se denomina política pública a las decisiones transversales que regulan la actuación interna de los gobiernos y que están destinadas a perfeccionar la gestión pública [3].
3. **Marcos jurídicos:** Conjunto de disposiciones, leyes, reglamentos y acuerdos a los que debe apegarse una dependencia o entidad en el ejercicio de las funciones que tienen encomendadas [3].
4. **Códigos de buenas prácticas:** Fórmulas que han demostrado, por medio de la investigación y la evaluación, su eficacia y sostenibilidad, que producen resultados sobresalientes y que pueden ser aplicables y adaptables a otras situaciones [4].

III. Normatividad Internacional

Un tratado internacional es un acuerdo celebrado por escrito entre Estados, o entre Estados y otros sujetos de derecho internacional, como las organizaciones internacionales, y regido por el derecho internacional [5]. En este nivel, el documento que aborda el tema de la protección de datos y la privacidad, es la *Declaración Universal de Derechos Humanos*, a través de la resolución *A/HRC/20/L.13 Promoción, Protección y Disfrute de los Derechos Humanos en Internet*, la cual declara que los derechos humanos deben estar garantizados en el mundo digital de la misma forma que en el mundo físico.

Varios acuerdos internacionales reconocen el derecho a la privacidad. Por ejemplo, la *Declaración Universal de Derechos Humanos*, establece en su 12º artículo: "Nadie será sometido a interferencia arbitraria con su privacidad, familia, hogar o correspondencia, ni a ataques contra su honor y reputación. Toda persona tiene derecho a la protección de la ley contra tales interferencias o ataques [6]"

Por otra parte, la Asamblea General de las Naciones Unidas, a través del documento A/C.3/71/L.39 *El derecho a la privacidad en la era digital* [7] reconoce que un entorno abierto, seguro, estable, accesible y pacífico en el ciberespacio es sumamente importante para la realización del derecho a la privacidad en la era digital. Luego, reafirma el derecho a la privacidad establecido en el artículo 12 de la *Declaración Universal de Derechos Humanos*, y el artículo 17 del *Pacto Internacional de Derechos Civiles y Políticos*. Reconoce, además, la naturaleza abierta de internet y el rápido avance de las tecnologías de la información, y por ello afirma que los derechos de las personas también deben estar protegidos en internet, incluyendo el derecho a la privacidad. Exhorta a los estados a que respeten y protejan el derecho a la privacidad en el contexto de las comunicaciones digitales, y que adopten las medidas para poner fin a las violaciones de esos derechos. Adicionalmente deben cerciorarse de que sus leyes se ajusten a sus obligaciones en virtud del derecho internacional, y a que examinen sus procedimientos, prácticas y legislaciones relativos a la vigilancia y la intercepción de las comunicaciones y la recopilación de datos personales.

Según el derecho internacional, los estados deben respetar la privacidad de las personas, mientras se aseguran de que terceros no participen en comportamientos que puedan afectar arbitrariamente su privacidad, la obligación se extiende al contexto de las comunicaciones digitales y la recopilación de datos personales [2].

En la misma dirección, el artículo 11 del *Pacto Internacional de Derechos Civiles y Políticos* retoma el texto mencionado anteriormente y agrega que "toda persona tiene derecho a la protección de la ley contra tales interferencias o ataques [8]".

IV. Normatividad Regional

Además de los tratados internacionales, el debate sobre el derecho a la privacidad ha llevado a diversos países a generar legislaciones locales que protejan a los usuarios en este tema. Entre estas destacan el *convenio número 108 del Consejo de Europa* [9], la *Directiva 2002/58/CE del Parlamento Europeo y del Consejo* [10] y el *Reglamento General de Protección de Datos (RGPD)* [11] en Europa, así como la *Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA)* [12], la *Ley Federal de Transacciones Crediticias Justas y Exactas (FATCA)* [13] y el *Acta de Privacidad del Consumidor de California* [14]. Finalmente, se presenta la *Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)* [15] correspondiente a la legislación mexicana.

Los instrumentos mencionados se describen a continuación.

IV-A. Unión Europea

Uno de los primeros antecedentes en Europa es el *convenio número 108 del Consejo de Europa,* del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el cual destaca por ser el primer instrumento internacional legalmente vinculante adoptado en el ámbito de la protección de datos [9].

Además, en 2002 se aprobó la *Directiva 2002/58/CE del Parlamento Europeo y del Consejo*, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (directiva sobre la privacidad y las comunicaciones electrónicas) [10], que entre sus consideraciones, define *la esfera privada de los usuarios, que debe ser protegida*, de la siguiente manera:

"Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Los denominados «programas espía» (spyware), web bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios. Sólo debe permitirse la utilización de tales

dispositivos con fines legítimos y con el conocimiento de los usuarios afectados."

Por otro lado, la Unión Europea aprobó el 14 de abril del 2016 el *Reglamento General de Protección de Datos (RGPD)*, cuyos objetivos incluyen [11]:

- Armonizar las leyes de privacidad de datos en toda Europa.
- Proteger y potenciar la privacidad de los datos de todos los ciudadanos de la UE.
- Cambiar la forma en que las organizaciones de toda la región abordan la privacidad de los datos.

El RGPD incluye, en su artículo 78, la siguiente declaración:

"La protección de los derechos y libertades de las personas físicas sobre el procesamiento de datos personales requiere que se tomen las medidas técnicas y organizativas apropiadas para garantizar que se cumplan los requisitos del presente Reglamento. Para poder demostrar el cumplimiento de este Reglamento, el controlador debe adoptar políticas internas e implementar medidas que cumplan en particular los principios de protección de datos por diseño y protección de datos por defecto. Dichas medidas podrían consistir, entre otras cosas, en minimizar el procesamiento de datos personales, pseudonimizar los datos personales lo antes posible, la transparencia en relación con las funciones y el procesamiento de los datos personales, permitir que el interesado monitoree el procesamiento de los datos, permitiendo que el controlador cree y mejorar las características de seguridad ... "

IV-B. Estados Unidos

A diferencia de Europa, las leyes de los Estados Unidos de América son reconocidas por ser más laxas en cuanto a protección de datos, y en general protegen la información personal de sus ciudadanos del acceso exterior.

Una de estas leyes es la *Ley de Transferibilidad y Responsabilidad del Seguro Sanitario (HIPAA)* [12]. Esta ley federal crea protecciones para información relacionada con la salud individual. Específicamente, quién puede tener acceso a la información relativa a la salud de sus ciudadanos.

Por otro lado, la *Ley Federal de Transacciones Crediticias Justas y Exactas (FATCA)* [13], está diseñada para ayudar a proteger la información de crédito de los consumidores de los riesgos asociados con el robo de datos, no obstante su intención es prevenir que los contribuyentes estadounidenses utilicen cuentas financieras fuera de los EE.UU. con el fin de evadir impuestos.

Finalmente, el estado de California aprobó en 2018, el *Acta de Privacidad del Consumidor de California*, la cual se convirtió en la legislación más estricta en materia de protección de datos en el país. En ella, el usuario adquiere el derecho de pedir a una empresa que no comparta ni venda su información personal. Además, obtiene el control sobre la información personal que recopila una empresa y las responsabiliza de salvaguardar su información personal [14].

IV-C. Organización para la Cooperación de Desarrollo Económico

El 23 de septiembre de 1980, los países miembros de la OCDE acordaron las *Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales* [16]. Si bien el documento puede ser considerado como antiguo, ha servido como una de las guías para sentar las bases de la protección de datos personales en medios digitales. Mediante el documento mencionado, recomienda "que los países miembros tengan en cuenta en su legislación interna los principios relativos a la protección de la privacidad y las libertades individuales". Además, deben esforzarse por eliminar o evitar que aparezcan,en nombre de la protección de la privacidad, obstáculos injustificados para los flujos transfronterizos de datos personales. En esencia, este documento requiere que la información cumpla con los siguientes puntos.

- Obtención legal y justa.
- Uso sólo para el propósito originalmente especificado.
- Ser adecuada, relevante y no excesiva a su propósito.
- Correcta y actualizada.
- Accesible al sujeto.
- Almacenada de manera segura.
- Destruida una vez que haya cumplido su propósito.

V. Normatividad Mexicana

En México, el instrumento existente es la *Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)* [15], promulgada el 5 de julio de 2010. La LFPDPPP, define dato personal como cualquier información concerniente a una persona física identificada o identificable, y prevé una definicion de *dato sensible*, para aquello referente a datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

Este documento, establece en su artículo 1º, lo siguiente:

"La presente Ley de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la determinación de regular su tratamiento legítimo, controlado e informado, un efecto de proteger la privacidad y el derecho a la autodeterminación informativa de las personas ".

Además, se establecen los principios de protección de datos personales, las autoridades reguladoras y las sanciones aplicables en caso de no cumplirse con las disposiciones establecidas. Y aunque reconoce a los datos personales como un *insumo de la economía digital*, no establece directrices específicas para el entorno de las tecnologías de la información.

El artículo 112 del reglamento de la LFPDPPP considera el tratamiento automático de la información, e invoca la obligación del responsable del almacenamiento de datos de informar al titular el tratamiento de los mismo, lo cual es aplicable en sistemas automatizados de tratamiento de datos. Sin embargo, el texto carece de fuerza ante la recolección de datos que hacen en Internet las empresas privadas con establecimientos en otros países. De esta forma, de frente al

desarrollo de nuevas tecnologías y maneras de procesar, analizar, almacenar y utilizar los datos personales, el reglamento se vuelve obsoleto.

VI. Conclusiones

Como se ha visto, la privacidad ha sido abordada en varios instrumentos legales con el objetivo de garantizar la protección de los datos de los usuarios, y con ello su seguridad. Sin embargo, uno de los principales retos es la dificultad de aplicar estas leyes al contexto digital, bien por interpretación o bien por jurisdicción. Por otro lado, es claro que se necesitan leyes acorde al contexto tecnológico, como el RGPD en la Unión Europea o el Acta de Privacidad del Consumidor de California, que consideren los aspectos relacionados con el diseño de infraestructura, hardware, código, y demás aplicables a los servicios que recaban datos y comercian con ellos. Además, se debe considerar el hecho de que los proveedores de los servicios no se ubican siempre en el lugar geográfico dónde la legislación tiene validez, por lo que deben diseñarse los instrumentos legales necesarios para proteger a los usuarios. Por otro lado, en el caso de México, el único instrumento que aborda el tratamiento de información personal es la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Sin embargo, no contempla de manera específica el caso de la información en Internet, los datos recabados por empresas asentadas en el extranjero ni las nuevas formas de procesar y almacenar información de este tipo. Por ello, es importante desarrollar una estrategia integral, alineada a los tratados internacionales de derechos humanos y civiles, que permita establecer un marco normativo que asegure a los usuarios el respeto a su privacidad, considerando el avance de las tecnologías de comunicaciones.

Agradecimientos

Los autores agradecen al Instituto Politécnico Nacional, que a través del Centro de Investigación en Computación, brindó el apoyo necesario para la realización de esta investigación, a través de los proyectos con número SIP 1917 y SIP 20196694.

Referencias

[1] D. Bradbury, "Anonymity and privacy: a guide for the perplexed," *Network Security*, vol. 2014, no. 10, pp. 10–14, 2014.
[2] A. Becerril, "Industria 4.0 vs leyes 0.9," INFOTEC, Octubre 2018.
[3] O. Montoya, "Diccionario jurídico." [Online]. Available: http://www.diccionariojuridico.mx/
[4] T. Ausín, "Buenas prácticas (códigos de)= best practices (codes of)," *EUNOMÍA. Revista en Cultura de la Legalidad*, no. 15, pp. 239–248, 2018.
[5] U. E. y. C. Ministerio de Asuntos Exteriores. Tratados internacionales. [Online]. Available: http://bit.do/e7Rw8
[6] U. G. Assembly, "Universal declaration of human rights," *UN General Assembly*, vol. 302, no. 2, 1948.
[7] "El derecho a la privacidad en la era digital." [Online]. Available: https://acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf
[8] International covenant on civil and political rights. [Online]. Available: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[9] C. de Europa, "Convenio n° 108 del consejo de europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal," 1981.
[10] U. Europea, "Directiva 2006/24/ce del parlamento europeo y del consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la directiva 2002/58/ce, diario oficial de la unión europea," *DO L*, vol. 105, no. 13.04, 2006.
[11] Directive 95/46/ec (general data protection regulation). [Online]. Available: https://eugdpr.org
[12] H. C. Assistance, "Summary of the hipaa privacy rule," *Office for Civil Rights*, 2003.
[13] IRS. Foreign account tax compliance act (fatca). [Online]. Available: https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca
[14] "Home: California consumer privacy act." [Online]. Available: https://www.caprivacy.org/
[15] C. de Diputados, "Ley federal de protección de datos personales en posesión de los particulares," *Diario Oficial de la Federación, Distrito Federal*, 2010.
[16] O. for Economic Co-operation and Development, *OECD guidelines on the protection of privacy and transborder flows of personal data*. OECD Publishing, 2002.