Quaestio Iuris
vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

LA PROTECCIÓN DE LOS DATOS PERSONALES EN EL ENTORNO DIGITAL. LOS ESTÁNDARES DE PROTECCIÓN DE DATOS EN LOS PAÍSES IBEROAMERICANOS

Adriana Margarita Porcelli[1]

Resumen
El notorio incremento de Internet y de las redes sociales ha generado un escenario en el que cada vez más datos personales son recolectados, almacenados y analizados, generando incluso nuevos datos a partir de ese tratamiento de los que el individuo en el que se originó la información desconoce totalmente. Los datos están empezando a hacer usados y reutilizados para los más diversos propósitos, muchos de los cuales puede ser perjudiciales para su titular. Por tanto, resulta necesario actualizar el significado del derecho a la privacidad en una economía digital, en la que la protección de los datos personales se ha convertido en una pieza fundamental, así como proporcionar un marco jurídico integral y tuitivo. A tales efectos, el objetivo del presente trabajo consiste en analizar el significado actual del derecho a la privacidad en una economía digital y las pautas de regulación jurídica establecidas en los Estándares de Protección de Datos en los Estados Iberoamericanos. Para cumplir con dicho objetivo, la metodología se basó, en primer lugar, en la delimitación y actualización del marco conceptual para posteriormente analizar los diferentes principios adoptados en los Estándares de Protección de Datos en los Estados Iberoamericanos.

Palabras clave: Datos Personales – Entorno Digital - Derecho – Estándares de Protección – Iberoamérica.

[1] Abogada (Universidad de Buenos Aires). Magíster en Relaciones Internacionales (Universidad Maimónides). Diploma en Derechos Económicos, Sociales y Culturales (Universidad Nacional de la Patagonia San Juan Bosco) Cursando la Actualización en Derecho Informático. (UBA)
Investigadora. Profesora Adjunta Ordinaria de Derecho Internacional Privado, de Derecho Internacional Público, de Estudio de la Constitución Nacional y de los Derechos Humanos y de Legislación Sanitaria. Miembro de Comisiones de Plan de Estudio de las carreras de Ingeniería Agronómica y Tecnicatura Universitaria en Inspección de Alimentos y del Comité Académico de Bioética. Miembro Titular de Comisiones Asesoras del Consejo Superior y del Consejo de Ciencias Sociales (Universidad Nacional de Luján). Universidad Nacional de Luján. Departamento de Ciencias Sociales. Argentina. E-mail: adporcelli@yahoo.com.ar

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

INTRODUCCIÓN

En el ciberespacio los consumidores convierten sus amistades, deseos, intereses emociones, preguntas y búsquedas en datos que luego son procesados para determinar patrones de consumo, sin evidenciar el real poder de ellos ya que están dispuestos a entregarlos para recibir un servicio en línea. A lo complejo del tema debe agregarse la necesidad de coordinación internacional por tratarse de asuntos que trascienden las fronteras nacionales.

En 2017, cerca de 4.000 millones de personas -más de la mitad de la población mundial- utilizaba Internet y un 56% lo hacía con suscripciones a servicios móviles. Por otra parte, el 61% de las suscripciones móviles operaban sobre redes 3G o 4G y durante el 2017 se descargaron 175.000 millones de aplicaciones de las que se utilizaron activamente alrededor de 40 en cada teléfono inteligente.

A principios de 2018 se registraban más de 5.000 millones de usuarios únicos de telefonía móvil, de los cuales 57% utilizaba teléfonos inteligentes. En enero de 2018, más de 3.000 millones de personas- el 42% de la población mundial- usaban mensualmente las redes sociales, especialmente mediante dispositivos móviles. En tanto, el uso de plataformas de comercio electrónico para comprar bienes de consumo creció hasta alcanzar los 1.800 millones de compradores- el 23% de la población mundial- en línea a nivel mundial. (COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE – CEPAL, 2018, p. 19, 20)

El poder de los datos masivos combinados, con inteligencia artificial, ha demostrado la increíble capacidad de predicción del comportamiento humano y modificarlo. Redes sociales como Facebook o Twitter permiten conocer los intereses de millones de personas en tiempo real, los estímulos a los que responden, momento de conexión, sitios visitados, bienes adquiridos, con quiénes interactúan y más. Al cruzar esa enorme cantidad de datos con las que tienen, por ejemplo, las tarjetas de crédito o los resultados electorales, se puede medir casi todo. Los datos están empezando a hacer usados y más que usados, reutilizados, porque no solo se utilizan para el fin que fueron recolectados sino para los más variados propósitos, como ser la generación de perfiles (*profiling*), la manipulación, la monitorización y selección de sujetos por su conducta (*behavioural targeting*) y las valoraciones basadas en decisiones automatizadas que pueden perjudicar seriamente a las personas.

Todas estas tecnologías, denominadas actualmente disruptivas, debe ser reguladas efectivamente por el derecho, reconfigurando el concepto del derecho a la privacidad y el

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

significado de lo íntimo, que en la actualidad ya no es el mismo que en las décadas anteriores y otorgar un marco jurídico adecuado y universal debido a que el ciberespacio no reconoce fronteras territoriales.

El notorio incremento de la economía digital ha generado un escenario en el que cada vez más datos de las personas son recolectados, almacenados y analizados, generando incluso nuevos datos a partir de ese tratamiento de los que el individuo en el que se originó la información desconoce totalmente. Según el informe de la Asociación por los Derechos Civiles "El sistema de protección de datos personales en América Latina: Oportunidades y desafíos para los derechos humanos", no se trata solo de datos o contenido que el sujeto genera de manera consciente, sino también de aquellos datos que genera con cada movimiento que realiza en línea y que por lo general desconoce y está más allá de su control. (ASOCIACIÓN POR LOS DERECHOS CIVILES – ADC, 2017, p.34)

El presente trabajo consiste en analizar el significado del derecho a la privacidad en la economía digital y las pautas de regulación jurídica establecidas en los Estándares de Protección de Datos en los Estados Iberoamericanos. A tales efectos, comprende dos partes: la primera delimita el marco conceptual y segunda analiza comparativamente los diferentes principios adoptados en su articulado.

MARCO CONCEPTUAL. DERECHO A LA PRIVACIDAD, A LA PROTECCIÓN DE DATOS PERSONALES Y A LA AUTODETERMINACIÓN INFORMATIVA EN LA ERA DIGITAL

En menos de una década, las redes digitales globales se convirtieron en poderosos medios de comunicación y de difusión de lo íntimo por los cuales circulan textos e imágenes en las más diversas lenguas y culturas. Contenidos que son permanentemente elaborados y reelaborados, leídos y releídos, modificados e intervenidos, olvidados o ignorados por millones de usuarios de todo el mundo. En ese contexto, la exposición de la intimidad, mejor dicho la autoexposición de las experiencias privadas, cobra una magnitud inimaginable. El usuario sube a Internet fotos, videos caseros, muchas veces de sus experiencias más íntimas, estamos frente al "show del yo", que conduce al impulso irrefrenable de "hacerse visible". El consumidor asiste a su propio espectáculo y lo ansía como meta superior. (SIBILIA, 2008, p. 9,10)

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

En el corazón de las redes sociales está el intercambio de información personal, los usuarios están felices de poder revelar detalles íntimos de sus vidas privadas e intercambiar fotografías. Todo se expone en la Red. Además, la mayor parte de la vida social se encuentra mediatizada electrónicamente, vale decir, se desarrolla en compañía de una computadora, un iPod o un celular, y los jóvenes no poseen ni el más mínimo margen de maniobra o elección, sino que se trata de una cuestión de tómalo o déjalo, de lo contrario, sufrirían una suerte de muerte social. (MARTÍNEZ & PORCELLI, 2016, p. 108)

La intimidad es reconocida por el derecho internacional de los derechos humanos, a saber, en el artículo 12 de la Declaración Universal de Derechos Humanos, en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, en el artículo 16 de la Convención sobre los Derechos del Niño y en el artículo 14 de la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares. Todos estos instrumentos internacionales entienden el derecho humano a la privacidad en el sentido que nadie debe ser objeto de injerencias arbitrarias o ilícitas en su vida privada, su familia, su domicilio o su correspondencia y el derecho a su protección. También reconocen que el ejercicio del derecho a la privacidad es importante para materializar el derecho a la libertad de expresión y a abrigar opiniones sin injerencias. En el ámbito americano, dicho derecho se encuentra receptado en el artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre y en el artículo 11 de la Convención Americana de Derechos Humanos de 1969. En igual sentido el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, el artículo 17 de la Carta Árabe de Derechos Humanos y el artículo 10 del Capítulo Africano: Carta sobre los Derechos y el Bienestar del Niño.

Sin embargo, hacer efectivo este derecho en el ámbito digital es, cada vez más, una ilusión. En el año 2014, Facebook modificó en secreto su algoritmo de difusión de noticias para investigar las emociones de unos 700.000 usuarios. La red social argumentó que el experimento fue legal porque los usuarios aceptaron de manera tácita su participación en esta clase de eventos al aprobar los términos de uso y servicio. (BBC MUNDO, 2014)

Por tanto, resulta necesario actualizar el significado del derecho a la privacidad en una economía digital, en la que la protección de datos personales se ha convertido en una pieza fundamental, ya que busca proteger la denominada identidad digital.

Se entiende por tal concepto a

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

> la información asociada a las actividades que los usuarios llevan a cabo en el ciberespacio, resultante de la interacción con otros usuarios, organizaciones o servicios en Internet, donde generalmente se trata de datos personales que suelen ser concedidos a terceros. (MENDOZA, 2017)

Sin embargo, no existe unanimidad en cuanto a la veracidad de tal concepto. Para algunos doctrinarios, es incorrecto hablar de identidad digital ya que una persona sólo puede tener una identidad real pero puede crear varias digitales, dependiendo de los ámbitos digitales en los cuales se relaciona (redes sociales, foros, servicios de mail, blogs, entre otros) Además la universalidad de datos que conforman la identidad real siempre encuentran correlato con una persona, existe la posibilidad de encontrar identidades digitales "vacías" es decir, que no existe una persona natural que se vincule realmente con esa universalidad. En consecuencia prefieren hablar de imagen digital, como la proyección de una persona en entornos digitales y no la identidad en sí de la persona. (LICEDA, 2011, p. 301, 302)

Por otro lado, el derecho a la protección de datos personales se ha conceptualizado en algunos países Iberoamericanos, legislativamente o jurisprudencialmente, como un derecho autónomo y de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y que tiene por objeto salvaguardar el poder de disposición y control que tiene todo individuo con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones. Es importante destacar que resguardando el derecho al tratamiento de los datos personales se garantiza y protege otros derechos humanos, los cuales se reconocen como indivisibles e interdependientes unos con otros que pueden verse afectados en virtud de intrusiones ilegales o arbitrarias, incluso aquellas derivadas del tratamiento de datos personales.

Lo que sí se reconocen nuevos derechos, acordes con las problemáticas actuales:

1) Derecho al olvido digital: como la facultad de las personas de solicitar a las empresas que borren sus datos personales en determinadas circunstancias, por ejemplo, cuando la información es irrelevante para los propósitos iniciales o cuando el dueño de los datos retira su consentimiento.

2) Derecho de oponerse a la elaboración de perfiles: lo que significa que las personas podrán oponerse a que sus datos personales se procesen o sean utilizados para la elaboración de perfiles en determinadas circunstancias.

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

3) Derecho a la portabilidad de datos: entendido como la facultad de las personas de obtener una copia de sus datos personales de la empresa que procesa su información en un formato común y legible.

4) Autodeterminación informativa: la facultad de toda persona para ejercer control sobre la información personal que le concierne.

LA PROTECCIÓN DE LOS DATOS PERSONALES EN LAS NACIONES UNIDAS

En este contexto, el Consejo de Derechos Humanos de las Naciones Unidas, en la Resolución del 24 de marzo de 2015 "El derecho a la privacidad en la era digital" creó la figura de un Relator especial sobre el derecho a la privacidad en la era digital, por un periodo inicial de tres años. (ORGANIZACIÓN DE LAS NACIONES UNIDAS-ONU, 2015)

Al año siguiente, la Asamblea General de las Naciones Unidas en su Septuagésimo primer período de sesiones adoptó, el 19 de diciembre de 2016, la Resolución N° 71/ 199, denominada "El derecho a la privacidad en la era digital", resaltando que el rápido ritmo del desarrollo tecnológico permitía a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones y, al mismo tiempo, incrementaba la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos y que si bien los metadatos aportaban beneficios, algunos tomados en conjunto, podían revelar información personal e indicaban el comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona. Tales circunstancias motivaron su preocupación ya que con frecuencia las personas no daban su consentimiento libre, explícito y fundado a la venta o a la reventa múltiple de sus datos personales. En consecuencia, exhortó, por un lado, a todos los Estados a elaborar o mantener y a aplicar una legislación adecuada, con sanciones y recursos eficaces con el objeto de proteger a las personas de las violaciones y transgresiones del derecho a la privacidad. En concreto referido a la recopilación y al tratamiento ilegal y arbitrario, la retención o el uso de datos personales por particulares, gobiernos, empresas y organizaciones privadas. Y, por otro lado, a las empresas a cumplir con la responsabilidad de respetar los derechos humanos, de conformidad con los Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en Práctica del Marco de las Naciones Unidas para "Proteger, Respetar y Remediar" e informar a los usuarios sobre la recopilación, el uso, el intercambio y la retención de los datos que puedan afectar su derecho a la privacidad. (ONU, 2016)

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

En marzo de 2017, Joseph Cannataci, Relator Especial de las Naciones Unidas, presentó al Consejo de Derechos Humanos, un informe denunciando la actual legislación de vigilancia y llamando a los Estados a respetar la privacidad como un derecho universal en la era digital.

El Relator observó que la vigilancia gubernamental merecía más atención que nunca ya que, en general, las leyes fueron redactadas para legitimar prácticas que nunca deberían haberse implementado. Además enfatizó que no apoyaba la legislación actual destinada a regular la vigilancia, ya que eran ineficaces y desproporcionadas frente a algunas medidas extremadamente intrusivas interpuestas por las nuevas leyes de vigilancia en Francia, Alemania, el Reino Unido y los Estado Unidos. Califica a tales medidas como una "política de gestos" por parte de los funcionarios públicos, cuya intención obedecía a demostrar que estaban haciendo algo, incluso si las leyes realmente no funcionaban en la práctica. Criticó la manipulación del miedo al terrorismo por parte de las autoridades, instándolos a desistir de "jugar la carta del miedo" y a mejorar la seguridad mediante medidas proporcionadas y efectivas, no con leyes intrusivas indebidamente desproporcionadas. Finalmente destacó la naturaleza universal del derecho a la privacidad, instando a los Estados a garantizar que tanto la privacidad a nivel nacional como internacional se respete como un derecho verdaderamente universal, especialmente con respecto a la vigilancia llevada a cabo en Internet. (UNITED NATIONS HUMN RIGHTS – OHCHR, 2017)

En virtud de la solicitud por parte del Consejo de Derechos Humanos al Alto Comisionado de las Naciones Unidas, para que elabore un informe clarificando e identificando los principios, estándares y buenas prácticas para la promoción y protección de los derechos humanos en la era digital incluida la responsabilidad de las empresas, dicho organismo, luego de haber recibido más de 60 contribuciones por múltiples actores, incluyendo los Estados miembros, organizaciones intergubernamentales, instituciones nacionales de derechos humanos, organizaciones de sociedad civil, empresas, académicos y expertos independientes, publicó el 3 de agosto de 2018 el Informe "*The right to privacy in the digital age*". En el mismo se destaca el avance de la tecnología basada en la explotación de datos vinculados a la vida de las personas en los ámbitos sociales, culturales, económicos y políticos de las sociedades modernas, siendo el sector privado el principal promotor de ellas.

Comienza analizando los riesgos sufridos actualmente por el derecho a la privacidad en el ciberespacio ya que se ve comprometido cuando la información sobre una persona es examinada o utilizada tanto por un ser humano como por un algoritmo. El simple hecho que se

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

generen y reúnan datos relativos a la identidad, la familia o la vida de una persona ya afecta a su derecho a la privacidad, pues pierde en cierta medida el control sobre una información que podría poner en riesgo su vida privada. Las injerencias solo son admisibles si no son arbitrarias o ilegales, vale decir, conforme con los principios generales de legalidad, necesidad y proporcionalidad y la legislación pertinente deben especificar con detalle las circunstancias precisas en que podrán autorizarse esas injerencias. El derecho a la privacidad es fundamental para el goce y el ejercicio de los derechos humanos dentro y fuera de Internet.

La implementación de tecnologías que conllevan un manejo intensivo de datos, como el *Big Data* y la inteligencia artificial, amenazan con crear un entorno digital intrusivo en donde los Estados y las empresas pueden desarrollar actividades de vigilancia, analizar, predecir e incluso manipular el comportamiento de las personas en un nivel sin precedentes.

A lo largo del documento se destacan las modernas tendencias y preocupaciones en cuanto a las injerencias en la privacidad. Por un lado, desarrolla el uso creciente de los datos personales por parte de los Estados y de las empresas enumerando las siguientes prácticas:

1) Aumento de la huella digital: las computadoras personales, los teléfonos y relojes inteligentes, los medidores de actividad física, los dispositivos y sensores interconectados instalados en los llamados hogares y ciudades inteligentes recopilan inmensos flujos de datos sobre miles de millones de personas. Esta información que se reúne y utiliza es enorme en alcance y profundidad, y abarca toda la vida privada incluidos los informes médicos, pautas de conducta, culturales, políticos, económicos y financieros, muchos de ellos recabados sin el conocimiento de las personas afectadas y sin su consentimiento válido.

2) Intercambio y fusión de datos: tanto las empresas como los Estados intercambian y fusionan constantemente datos personales procedentes de diversas fuentes y bases de datos, Por tanto, los individuos se ubican en una posición de indefensión, ya que resulta prácticamente imposible llevar un seguimiento de la información y aún más controlar las múltiples formas en que puede ser utilizada.

3) Datos biométricos: cada vez se utiliza más los sistemas basados datos biométricos, como el ADN, la geometría facial, la voz, los patrones de la retina o el iris y las huellas dactilares. El informe demuestra su preocupación por la creación de enormes bases de datos centralizadas que almacenan ese tipo de información para una amplia variedad de fines, desde la seguridad nacional, el control de la migración, tanto en las fronteras como dentro de los países y la investigación penal hasta la identificación de personas para la prestación de servicios esenciales,

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

como servicios sociales, financieros o educativos. Estos son datos particularmente delicados, ya que están vinculados a una persona concreta y a su vida, y pueden ser objeto de graves vulneraciones. Teniendo en cuenta esos riesgos, aconseja que, al recopilar datos biométricos, se debería prestar especial atención a los principios de necesidad y proporcionalidad.

4) Aumento de la capacidad de análisis: el análisis de macrodatos y la inteligencia artificial permiten a los Estados y a las empresas obtener información cada vez más específica sobre la vida de las personas, hacer deducciones sobre sus características físicas y mentales, crear perfiles de personalidad detallados, evaluarlas, clasificarlas y, en última instancia, adoptar decisiones, a menudo automatizadas, acerca de ellas. En este punto, señala, con gran preocupación, la relación existente entre la recopilación y el análisis ilegales de datos y las campañas de captación de votantes.

Por otro lado, detalla la vigilancia e interceptación de las comunicaciones por los Estados realizada por medio de los siguientes mecanismos:

1) Vigilancia a gran escala: muchos Estados continúan con actividades secretas de vigilancia e interceptación de las comunicaciones a gran escala, y recopilando, almacenando y analizando datos de todos los usuarios en una amplia gama de medios de comunicación bajo la justificación de proteger la seguridad nacional. Sin embargo, el Tribunal Europeo de Derechos Humanos viene señalando que un sistema de vigilancia secreta puede socavar o incluso destruir la democracia con el pretexto de defenderla.

2) Acceso a los datos de los usuarios de las empresas: los Estados suelen recurrir a las empresas para recopilar e interceptar datos personales. Algunos Estados obligan a los proveedores de servicios de telecomunicaciones e Internet a darles acceso directo a los flujos de datos que circulan a través de sus redes. Muchas leyes obligan a las empresas a recopilar y a almacenar de manera indiscriminada la totalidad de los datos de tráfico de todos los abonados y usuarios en todos los medios de comunicación electrónica, excediendo los límites de lo necesario y proporcional.

3) Piratería informática (hacking estatal): algunos Gobiernos recurren con mayor asiduidad a programas informáticos de interceptación maliciosa que permiten la recopilación indiscriminada de todo tipo de comunicaciones y de datos-cifrados o no- así como el acceso remoto y secreto a los dispositivos personales, así como a los datos almacenados en ellos, habilitando su manipulación. Es común algunos intentos reiterados de los Estados de debilitar la tecnología de cifrado y limitar el acceso a las herramientas de anonimato ya que piden que se introduzcan

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

puertas traseras obligatorias en las comunicaciones cifradas, exigen a los proveedores de servicios de este tipo de comunicaciones que proporcionen copias de las claves de cifrado o incluso prohíben o bloquean ciertas aplicaciones de comunicación segura, en particular los servicios de mensajería cifrada y redes virtuales privadas y anónimas, afectando gravemente los derechos humanos.

4) Intercambio de información de inteligencia: el intercambio de inteligencia constituye una práctica habitual en los gobiernos sin sujeción a un marco jurídico ni a una supervisión adecuada.

5) Acceso transfronterizo a los datos de las empresas: el informe destaca los esfuerzos encaminados por crear mecanismos jurídicos que faciliten el acceso de los Estados a la información personal almacenada en los servidores de las empresas en el extranjero. No obstante, ese acceso puede resultar en el debilitamiento o la elusión de las garantías procesales, como el requisito de autorización por un órgano independiente y el establecimiento de mecanismos de supervisión adecuados.

El informe brinda una serie de guías para abordar algunas de los desafíos que enfrenta el derecho a la privacidad en la era digital. Además, detalla la responsabilidad del Estado y la obligación de respetar y proteger el derecho a la privacidad en la era digital y de establecer salvaguardias adecuadas y una supervisión eficaz. Entre las medidas a adoptar enumera las siguientes:

1) Marco general de protección contra injerencias indebidas: existe un consenso mundial acerca de la necesidad de unas normas mínimas que rijan el tratamiento de los datos personales por los Estados, las empresas y otros agentes del sector privado que garantizan un nivel mínimo de protección de los datos personales. Entre los instrumentos y directrices internacionales que reflejan estos avances están los Principios Rectores sobre la reglamentación de los ficheros computadorizados de datos personales de 1990; Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, suscripto en la ciudad de Estrasburgo, República Francesa, el día 28 de enero de 1981, y el Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las autoridades de control y a los flujos transfronterizos de datos, suscripto en la ciudad de Estrasburgo, República Francesa, el día 8 de noviembre de 2001 (recientemente aprobado por Argentina, el 2 de enero de 2019) ; las Directrices sobre Privacidad de la Organización de Cooperación y Desarrollo Económicos, de 1980, actualizadas en 2013; la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

(Convención de Malabo), de 2014; la resolución de Madrid de la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad; y el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico, de 2015, entre otros. Esas normas, en particular el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, han servido de base para la elaboración de los marcos de protección de datos de muchos Estados y pueden utilizarse para el diseño de instrumentos de política adecuados. Estos instrumentos contienen una serie de principios, derechos y obligaciones fundamentales que son coincidentes con los Estándares Iberoamericanos.

2) Salvaguardias de procedimiento y supervisión de la vigilancia y la interceptación de las comunicaciones: en cuanto a las salvaguardias, el Relator Especial sobre el derecho a la privacidad remarcó la falta generalizada de legislación en las actividades de vigilancia. Por tal motivo, se calificó como imperioso el dictado de un marco jurídico bajo los siguientes criterio mínimos:

a) acceso público: se justifican las facultades de vigilancia secreta solamente en la medida en que sean estrictamente necesarias para lograr un objetivo legítimo y que cumplan con el requisito de proporcionalidad y se limiten a prevenir o investigar los delitos o amenazas más graves;
b) deben ser suficientemente precisas: las referencias vagas a la "seguridad nacional", no pueden considerarse disposiciones suficientemente claras. La vigilancia debe basarse en sospechas razonables y toda decisión que la autorice debe ser suficientemente específica;
c) en cuanto a su alcance, el marco jurídico de la vigilancia debe abarcar las solicitudes presentadas por los Estados a las empresas, el acceso a información conservada extraterritorialmente o al intercambio de información con otros Estados;
d) medidas de piratería selectivas: los gobiernos deben ser sumamente cautelosos y recurrir a ellas únicamente en circunstancias excepcionales para investigar y prevenir los delitos o amenazas más graves y sujetas a la orden del poder judicial;
e) deben estar autorizadas y supervisadas por organismos independientes, preferiblemente por el poder judicial, en todas las etapas;
f) deben ser transparentes: aplica el principio de transparencia ya que el informe considera que el debate público es esencial para comprender las ventajas y limitaciones de las técnicas de vigilancia y las personas sometidas a ella deben ser

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

informadas, además de tener derecho a modificar o eliminar información personal no pertinente, siempre y cuando no sea necesaria para llevar a cabo una investigación en curso o pendiente.

Seguidamente se refiere a la responsabilidad de la empresas de aplicar la debida diligencia en materia de derechos humanos al identificar y evaluar las consecuencias de sus actividades. Como parte de la puesta en práctica de los compromisos políticos contraídos en virtud de los Principios Rectores, el sector de las TICs ha elaborado directrices para la aplicación de políticas de derechos humanos. Entre esas iniciativas están los Principios de Libertad de Expresión y Privacidad de *Global Network Initiative* (Principios de la GNI) y los Principios Rectores del Grupo de Diálogo de la Industria de las Telecomunicaciones. Especial mención merece el Índice de Responsabilidad Empresarial de *Ranking Digital Rights Corporate,* el cual evalúa una serie de empresas de Internet, telefonía móvil y telecomunicaciones centrándose específicamente en sus compromisos de divulgación y sus políticas en lo que respecta a la libertad de expresión y la privacidad. Este podría ser un instrumento útil para pedir responsabilidades a las empresas por el impacto de sus actividades en los derechos de los usuarios. (HUMAN RIGHTS COUNCIL, 2018)

El Índice de Responsabilidad Empresarial 2018, clasificó a 22 compañías evaluando la transparencia en cuanto al cumplimiento de los compromisos y las políticas que afectan la libertad de expresión y la privacidad. Midió las políticas de la empresa matriz, la operadora y las de los servicios seleccionados. En cuanto a las empresas de Internet y ecosistemas móviles, el ranking lo encabeza Google, seguida por Microsoft, Juramento, Facebook y Twiter. Y en lo que respecta al rubro telecomunicaciones, lo lidera Vodafone, después AT&T, Telefónica, Naranja y América Móvil. Finalmente de la comparación 2017 a 2018, entre las empresas que mejoraron en relación con el Índice 2017 se encuentran, en primer lugar, Apple, seguida por Telefónica, Twiter, Vodafone, Baidu, Facebook, Orange, Samsung, Oath, AT&T, Google. (RANKING DIGITAL RIGHTS, 2018, p. 19, 21)

Retomando con el análisis del Informe, en el último capítulo, el Alto Comisionado recomienda a los Estados que adopten una legislación sólida, rigurosa y exhaustiva sobre privacidad, en particular sobre protección de datos; que velen por que los sistemas que emplean un gran volumen de datos, incluidos los que implican la recopilación y conservación de datos biométricos, solo se utilicen en casos que sean necesarios y proporcionales para lograr un fin legítimo; que establezcan autoridades independientes para supervisar las prácticas del Estado y

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

el sector privado; que adopten medidas para aumentar la transparencia y la rendición de cuentas en la adquisición de tecnologías de vigilancia por los Estados; que velen para que todas las víctimas de violaciones del derecho a la privacidad tengan acceso a recursos eficaces, incluso en los casos transfronterizos.

Y a las empresas que hagan todos los esfuerzos necesarios para cumplir con su responsabilidad de respetar el derecho a la privacidad y los demás derechos humanos. Como mínimo, las compañías deben hacer plenamente efectivos los Principios Rectores sobre las Empresas y los Derechos Humanos; traten de asegurar un alto nivel de seguridad y confidencialidad en las comunicaciones que transmitan y en los datos personales que recopilen, almacenen o traten de otro modo; cumplan los principios de privacidad fundamentales mencionados en el informe y reparen, mediante procedimientos legítimos y mecanismos de reclamación eficaces a nivel operacional, todo daño que hayan provocado o contribuido a provocar.

ESTÁNDARES DE PROTECCIÓN DE DATOS EN LOS PAÍSES IBEROAMERICANOS

En el marco del XV Encuentro Iberoamericano de Protección de Datos, celebrado del 20 al 22 de junio de 2017 en Santiago de Chile, la Red Iberoamericana de Protección de Datos (RIPD o Red) ha aprobado y presentado oficialmente los llamados "Estándares de Protección de Datos de los Estados Iberoamericanos". Consisten en un conjunto de directrices orientadoras cuyo objetivo reside en proporcionar un marco normativo que guíe los proyectos de ley de protección de datos personales en la región iberoamericana en aquellos países que aún no cuentan, en sus ordenamientos jurídicos, con una legislación, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes. Forman parte del *soft law* – ley blanda- ya que no obstante no ser vinculantes, tienen relevancia jurídica y manifiestan consensos internacionales que independientemente de su valor jurídico se incorporan al discurso internacional y producen ciertos efectos que repercuten de diferentes formas en la formación, desarrollo, interpretación, aplicación y cumplimiento del derecho internacional, tanto en el ámbito interno de los Estados como en el propio seno del derecho internacional.

Parte de la base que la protección de los datos personales de las personas naturales es un derecho fundamental reconocido en la mayoría de las Constituciones Políticas de los Estados Iberoamericanos. Así, por ejemplo fue instituido en la Constitución de Portugal de 1976 (art. 35)

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

y en la de España de 1978 (art. 105, "b"). Asimismo, Gran Bretaña y Estados Unidos poseen similares sistemas de control por parte de los ciudadanos con relación a los bancos de datos. En Latinoamérica, en Argentina, la reforma constitucional de 1994 establece la acción de habeas data en forma independiente a la acción de amparo y la Constitución de la República Federativa de Brasil, introdujo en su artículo 5º el habeas data junto con el denominado *mandado de injunçao* (mandato de ejecución), que daba operatividad a la norma, cuando a falta de disposiciones reglamentarias se tornara complicado el ejercicio de los derechos y libertades constitucionales. (MORELLO, 1998, p. 240, 241).

A título informativo, Argentina, Chile y México cuentan con leyes sobre protección de datos personales. La ley argentina data del año 2000, la chilena del año 1996, México cuenta con una ley específica para el sector privado del año 2010 y una ley aprobada en diciembre del 2016 específica para el sector público. Brasil no cuenta con una ley específica ni con un sistema de protección de datos personales. Pero contempla diversos tipos de datos personales en distintas leyes y normativas. Por ejemplo en la protección de datos de las telecomunicaciones, en la Ley General de Telecomunicaciones, en el Marco Civil de Internet y su decreto reglamentario, ley de interceptaciones, ley de organizaciones criminales, en el código Penal. También se encuentra referencias relativas a datos de los consumidores, de los datos financieros y de datos de salud en normativa específica de cada uno de estos sectores. En Argentina, el 3 de abril de 2018 obtuvo media sanción en la Cámara de Senadores el Anteproyecto de Ley de Protección de Datos Personales y Brasil también reconoció la necesidad de una ley comprensiva de protección de datos, y mediante un proceso de participación colectiva iniciado por el Ministerio de Justicia fue elaborado un proyecto de ley que fue presentado al Congreso en el 2016. (ADC, op.cit., p. 18)

Los estándares comprenden 45 artículo divididos en diez capítulos. El Capítulo I (Disposiciones generales) comprende del artículo 1 al 9; Capítulo II (Principios de protección de datos personales) abarca desde el artículo 10 al 23; Capítulo III (Derechos del titular) del artículo 24 al 32; Capítulo IV (Encargado) comprende los artículos 33 al 35; Capítulo V (Transferencias internacionales de datos personales) el artículo 36; Capítulo VI (Medidas proactivas en el tratamiento de datos personales) desde el artículo 37 al 41; Capítulo VII (Autoridades de control) el artículo 42; Capítulo VIII (Reclamaciones y Sanciones) el artículo 43; Capítulo IX (Derecho de indemnización) el artículo 44 y Capítulo X (Cooperación internacional) el artículo 45.

Disposiciones Generales

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

El objetivo principal de los Estándares (artículo 1) radica en establecer un marco común de principios y derechos de protección de datos que sirvan como modelo para las diferentes legislaciones nacionales de los Estados Iberoamericanos de forma que se garantice una tutela homogénea del derecho a la protección de datos personales en todos los Estados de la región, se facilite el flujo de los datos personales entre los mismos y más allá de sus fronteras y se desarrollen mecanismos para la cooperación internacional entre las autoridades de control y entidades internacionales en la materia. Reconocen como fuente y marco de referencia el nuevo Reglamento Europeo (UE) 2016/679 ("GDPR") vigente desde el 25 de mayo de 2018 e incluyen medidas muy similares a las consignadas en ella.

En el artículo 2 establece las definiciones de los términos utilizados en la misma, a saber:
1) Anonimización: consiste en la aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona.
2) Consentimiento: se considera dicho término como la manifestación libre, específica, inequívoca e informada de la voluntad del titular por la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.
3) Datos Personales: se entiende por tal cualquier información expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo concerniente a una persona física identificada o identificable. En este punto, es ilustrativo mencionar la nueva Resolución N° 4/2019 del 16 de enero del 2019 de la Agencia de Acceso a la Información Pública de Argentina que cataloga como dato personal a los sistemas de video vigilancia y la imagen de las personas. (ARGENTINA. AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, 2019)
4) Datos personales sensibles: son los que se refieren a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste, por ejemplo el origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona. La Resolución comentada *ut supra* considera que los datos biométricos son los datos personales derivados de un tratamiento técnico específico, referente a las características físicas, fisiológicas o conductuales de una persona, que permitan o confirmen su identificación única.

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

5) Encargado: es el prestador de servicios (persona humana, jurídica o autoridad pública) ajena a la organización del responsable, que trata datos personales a nombre y por cuenta de éste.
6) Exportador: persona natural o jurídica- de carácter público o privado-, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales.

En cuanto al ámbito de aplicación, diferencia el subjetivo, el objetivo y el territorial. Con respecto al sujeto pasivo, en el artículo 3, dispone que los Estándares se aplican a las personas naturales y jurídicas de carácter público o privado que se dediquen al tratamiento de datos personales en el ejercicio de sus actividades y funciones.
Por regla general, como sujeto activo se refiere a los datos personales de personas naturales, no obstante deja a criterio de la legislación interna de cada Estado la protección de los datos personales de las personas jurídicas. (artículo 4.2.)

El ámbito de aplicación objetivo comprende el tratamiento de datos personales en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización (artículo 4.1.)

Como excepciones a la aplicación de los estándares establece las siguientes situaciones:
1) si los datos personales están destinados exclusivamente a actividades dentro de la vida familiar de un individuo, en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como propósito una divulgación o utilización comercial.
2) si la información sea anónima, es decir, aquélla que no guarda relación con una persona natural identificada o identificable, así como los datos personales sometidos a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado. (artículo 4.4.)
A diferencia de los Estándares, la Resolución N° 4/2019 de Argentina expresamente aclara que aun en el caso que el dato anonimizado pueda recuperarse por ingeniería inversa u otra técnica que permita reidentificar el dato con una persona determinada igualmente deja de estar protegido pese a la posibilidad de asociar el dato con una persona, si para ello se requieren medidas o plazos desproporcionados o inviables. Es criticable la utilización en dicha norma del calificativo de desproporcionado o inviable por la incertidumbre que genera.
3) las categorías de datos personales expresamente establecidos en la legislación nacional de cada Estado (artículo 4.5.) para salvaguardar la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

cuestiones de interés público. Como mínimo, exige que dicha ley debe contener los siguientes ítems: la finalidad del tratamiento, las categorías de datos personales de que se trate, el alcance de las limitaciones establecidas, las garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas, la determinación del responsable o responsables, los plazos de conservación de los datos personales, los posibles riesgos para los derechos y libertades de los titulares y el derecho de los titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a sus fines. (artículo 6)

En cuanto al ámbito territorial, estos Estándares se aplican a los tratamientos efectuados en territorio de los Estados Iberoamericanos así como a responsables o encargados no establecidos en territorio de los Estados Iberoamericanos cuando las actividades del tratamiento están relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados Iberoamericanos; o con el control de su comportamiento en los Estados Iberoamericanos; o cuando le resulte aplicable la legislación nacional de un Estado, en virtud de la celebración de un contrato o del derecho internacional público (artículo 5.1.) Vale decir que le otorga efectos extraterritoriales regionales

Por establecimiento principal entiende el lugar de la administración central o principal del responsable o encargado, que implique el ejercicio efectivo y real de actividades de gestión (artículo
5.2.) En caso que el tratamiento de datos personales lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control es considerado como el establecimiento principal del grupo empresarial (artículo 5.3.)

Especial mención tienen los datos personales de los niños, niñas y adolescentes (artículo 8) ya que privilegia la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral y obliga a los Estados a la formación académica sobre el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades. El artículo 9 (Tratamiento de datos personales de carácter sensible) cierra este primer Capítulo. Por regla general, el responsable no podrá tratar datos personales sensibles, salvo que sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación; o en cumplimiento a un mandato legal; o que cuente con el consentimiento

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

expreso y por escrito del titular o que sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

Principios Rectores Adoptados en los Estándares

Los datos personales se han vuelto un activo central para las empresas y para una administración de gobierno más efectiva. Su manejo constituye una forma de adquirir poder económico y político por parte de empresas y gobiernos. Frente a esta situación, los individuos se encuentran en un estado de vulnerabilidad producto de una relación asimétrica. Por consiguiente, los Estándares, en el artículo 10 (Principios aplicables al tratamiento de datos personales) iniciando el Capítulo II, identifican los principios básicos que deben regir el tratamiento de datos personales, a saber: legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

Con respecto al principio de legitimación, el artículo 11, enumera una serie de supuestos según los cuales, el responsable está habilitado al tratamiento de los datos:

1) que el titular otorgue su consentimiento para una o varias finalidades específicas,

2) que el tratamiento sea necesario para el cumplimiento de una orden judicial o mandato fundado y motivado de autoridad competente;

3) que sea necesario para el ejercicio de facultades propias de las autoridades;

4) para el reconocimiento o defensa de los derechos del titular ante una autoridad;

5) para la ejecución de un contrato o precontrato en el que el titular sea parte;

6) para el cumplimiento de una obligación legal aplicable al responsable;

7) para proteger intereses vitales del titular o de otra persona;

8) por razones de interés público establecidas en ley o

9) para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular, en particular si se trata de un niño, niña o adolescente.

En los casos en que se exige el consentimiento del titular, en el artículo 12, detalla las condiciones para que dicho consentimiento sea válido. Pone en cabeza del responsable demostrar de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara, vale decir, siempre debe ser expreso y no acepta la forma tácita. es

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

decir, no debe dar lugar a ninguna duda o ambigüedad con respecto a la intención de la persona. Para que el consentimiento sea válido, la persona debe contar con suficiente información sobre los detalles concretos de los datos que se recopilarán, la forma en que se recopilarán, los fines del procesamiento y toda divulgación que pueda efectuarse. Con todas estas exigencias, lo que persigue es que la persona sea capaz de efectuar una elección real y se basa en el concepto de la "autodeterminación en lo que respecta a la información"

Además faculta al individuo a revocarlo en cualquier momento, para lo cual el responsable deberá contar con mecanismos sencillos, ágiles, eficaces y gratuitos.

Especial mención tiene el consentimiento de los niñas, niñas y adolescentes. En el artículo 13, exige la autorización de su representante legal o directamente la autorización del menor de edad si en el derecho interno de los Estados se ha establecido una edad mínima para que lo pueda otorgar directamente y sin representación alguna. A partir de la reforma del Código Civil y Comercial de Argentina, el artículo 26 de dicho cuerpo normativo, prescribe que la persona menor de edad ejerce sus derechos a través de sus representantes, pero si cuenta con edad y grado de madurez suficiente puede ejercer por sí mismo los actos que le son permitidos por el ordenamiento. Establece el principio de la "autonomía progresiva" y presume que el adolescente entre 13 y 16 años tiene aptitud para decidir por sí respecto de aquellos tratamientos que no resultan invasivos ni comprometen su estado de salud o provocan un riesgo grave en su vida o integridad física. (ARGENTINA. CÓDIGO CIVIL Y COMERCIAL DE LA NACIÓN -CCyC, 2014, p. 5)

Por el principio de licitud (artículo 14) el responsable debe tratar los datos en cumplimiento de lo dispuesto por el derecho interno, por derecho internacional y por los derechos y libertades de las personas. Conforme el de lealtad (artículo 15) el responsable tiene la obligación de privilegiar la protección de los intereses del titular y abstenerse de tratarlos a través de medios engañosos o fraudulentos. Considera desleales aquellos tratamientos que den lugar a una discriminación injusta o arbitraria contra sus titulares.

En virtud del principio de transparencia (artículo 16) el responsable deberá informarle al titular de los datos como mínimo: su identidad y datos de contacto; las finalidades del tratamiento de sus datos; las comunicaciones, nacionales o internacionales que pretenda realizar, incluyendo los destinatarios y las finalidades; los mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad. Toda esta

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

información debe ser suficiente y fácilmente accesible, así como redactarse en un lenguaje claro, sencillo y de fácil comprensión especialmente si se trata de niñas, niños y adolescentes.

En el artículo 17, principio de finalidad, prohíbe el tratamiento de los datos personales para finalidades distintas a las originales, salvo que se den las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

Según el principio de proporcionalidad (artículo 18) el responsable tratará únicamente los datos que resulten adecuados, pertinentes y limitados al mínimo necesario y por el principio de calidad (artículo 19) debe mantenerlos exactos, completos y actualizados, debiendo suprimirlos y eliminarlos de manera segura y definitiva cuando dejen de ser necesarios o en su caso, los someterá a un procedimiento de anonimización. En este caso, la legislación nacional puede establecer excepciones respecto al plazo de conservación de estos.

Es importante destacar que en virtud del principio de responsabilidad, el responsable debe implementar todos los mecanismos necesarios para el cumplimiento de los principios y obligaciones establecidas en los Estándares, así como rendirá cuentas sobre el tratamiento de datos personales al titular y a la autoridad de control (artículo 20). Además debe adoptar medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales (artículo 21: principio de seguridad). En caso de vulneración de seguridad (daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales) el responsable debe documentarla y notificar del suceso en un lenguaje claro y sencillo a la autoridad de control y a los titulares afectados por dicho acontecimiento, sin dilación alguna (artículo 22). Dicha notificación debe contener, al menos la naturaleza del incidente, los datos personales comprometidos, las acciones correctivas realizadas y las recomendaciones al titular para proteger sus intereses. Finalmente, el artículo 23 establece el principio de confidencialidad.

Derechos de los Titulares. Derechos ARCO

En el Capítulo II, artículo 24, reconoce expresamente los clásicos derechos de acceso, rectificación, cancelación, oposición (conocidos como derechos ARCO) así como otros nuevos derechos como el derecho a no ser objeto de decisiones individuales automatizadas (salvo excepciones), el derecho a la limitación del tratamiento y el derecho a la portabilidad.

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

Por el derecho de acceso, el titular de los datos personales tiene la facultad de tomar conocimiento de cualquier información relacionada con las condiciones generales y específicas de su tratamiento (artículo 25). Por el de rectificación (artículo 26) puede obtener la corrección de sus datos personales, cuando resulten ser inexactos, incompletos o desactualizados y por el de cancelación (artículo 27) solicitar la supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable. Es el derecho al olvido, que en la era informática cobra una dimensión más abarcativa. Según el Tribunal Constitucional Español, el derecho al olvido digital es una vertiente del derecho a la protección de datos personales frente al uso de la informática y es también un mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo. (ESPAÑA.TRIBUNAL CONSTITUCIONAL, 2018, p. 68425)

Textualmente afirmó que:

> el llamado 'derecho al olvido digital', que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos. Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas, 'posicionando' a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones. De admitirse esta tesis, se perturbarían gravemente los mecanismos de información necesarios para que los ciudadanos adopten sus decisiones en la vida democrática de un país. Pero dicho derecho sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse al tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos personales tales como el nombre y apellidos, haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, de modo que se distorsione gravemente la percepción que los demás ciudadanos tengan de su persona, provocando un efecto estigmatizador e impidiendo su plena inserción en la sociedad, inserción que se vería obstaculizada por el rechazo que determinadas informaciones pueden causar en sus conciudadanos. (ESPAÑA.TRIBUNAL CONSTITUCIONAL, 2018, p. 68415)

Además el titular puede oponerse al tratamiento de sus datos cuando tenga una razón legítima o el tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles. (artículo 28 derecho de oposición).

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

Ahora bien lo novedoso es que están expresamente receptados los siguientes derechos derivados de las nuevas tecnologías de la información y comunicación:

1. Derecho a no ser objeto de decisiones individuales automatizadas (artículo 29) ya que prohibe las decisiones que afecten significativamente al titular de los derechos personales basadas únicamente en tratamientos automatizados para evaluar, sin intervención humana, los aspectos personales o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

En esta última parte del artículo incluye las elaboraciones de perfiles o *profiling* que consisten en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a un individuo, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, siempre que produzcan efectos jurídicos o le afecte significativamente. Como ejemplo se puede mencionar la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. En sintonía, en Argentina, en el Código Civil y Comercial de la Nación, dentro del Capítulo 12 (Contratos Bancarios con Consumidores y Usuarios) artículo 1387 segundo párrafo obliga al banco, frente al rechazo de una solicitud de crédito por la información negativa registrada en una base de datos, a informar al consumidor en forma inmediata y gratuita el resultado de la consulta y la fuente de donde la obtuvo. Y la Resolución N° 4/2019 extiende la obligación al universo de todos los contratantes, no solo los contratos bancarios. (ABDELNABE VILA, 2019)

Como excepción a dicha prohibición, vale decir, los Estándares facultan el tratamiento automatizado de datos personales cuando sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable; esté autorizado por el derecho interno de los Estados; o bien, se base en el consentimiento demostrable del titular. Sin embargo, en este último caso tendrá derecho a obtener la intervención humana, recibir una explicación sobre la decisión tomada, expresar su punto de vista e impugnar la decisión, es decir ejercer el derecho de oposición. Finalmente, prohíbe el tratamiento automatizado de datos personales basados en datos sensibles, que impliquen algún tipo de discriminación en las personas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto.

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

2. Derecho a la portabilidad de los datos personales (artículo 30): en caso de tratamiento automatizado de datos personales o por medios electrónicos, el titular tiene derecho a obtener una copia de ellos, en un formato electrónico estructurado, de uso común y lectura mecánica, para seguir utilizándolos y, en su caso, transferirlos a otro responsable.

El Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE ha adoptado directrices sobre la aplicación del derecho a la portabilidad. Por ejemplo, considera que el concepto de datos facilitados por el interesado incluye los datos proporcionados de manera activa por el interesado y los datos observados (datos de ubicación, búsqueda, ritmo cardiaco, entre otros) pero no incluye, dentro de los datos sujetos al derecho a la portabilidad, a los datos inferidos o deducidos que hayan sido creados por el responsable de tratamiento a partir de los datos proporcionados por el interesado (como pueden ser los resultados algorítmicos). (ESPAÑA. AGENCIA ESPAÑOLA DE DATOS PERSONALES – AGPD, 2017, p. 24)

Justamente esta excepción esta receptada en los Estándares ya que el derecho a la portabilidad de los datos personales no procede si se trata de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

3. Derecho a la limitación del tratamiento de los datos personales (artículo 31): significa que, cuando el titular haya ejercido el derecho de oposición o rectificación, el tratamiento de datos personales se limita exclusivamente a su almacenamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado, o cuando el responsable ya no los necesite pero el interesado los precise para la formulación, el ejercicio o la defensa de reclamaciones.

Modalidad en el ejercicio de los derechos. La figura del Encargado

En el artículo 32 reglamenta la manera de ejercer todos los derechos desarrollados en los artículos precedentes. Fundamentalmente el responsable debe establecer medios y procedimientos sencillos, expeditos, accesibles y gratuitos y deja a cargo de la legislación nacional de los Estados el establecimiento de los requerimientos, plazos, términos y condiciones en que los titulares puedan ejercer sus derechos.

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

Además establece una serie de causales de improcedencia a su ejercicio, de manera enunciativa y no limitativa, como guía para las legislaciones locales, a saber:

1) cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público; o

2) para el ejercicio de las funciones propias de las autoridades; o

3) para el cumplimiento de una disposición legal; o

4) para el mantenimiento o cumplimiento de una relación jurídica o contractual; o

5) cuando el responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular.

También reconocen expresamente el derecho de los titulares y, en su caso el de sus sucesores, a presentar una reclamación ante la autoridad de control en caso de vulneración de sus derechos así como el derecho a ser indemnizado.

En el Capítulo IV regula la figura del encargado del tratamiento, como la entidad que trata los datos personales "sin poder alguno de decisión sobre el tratamiento" y en los términos fijados por el responsable. La relación entre el encargado y el responsable debe formalizarse en un contrato que deberá incluir como contenido mínimo el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento; el tipo de datos personales; las categorías de titulares, así como las obligaciones y responsabilidades del responsable y del encargado.

También detalla al menos las siguientes cláusulas generales relacionadas con los servicios del encargado, a saber:

1) realizar el tratamiento de los datos personales;

2) abstenerse de su tratamiento para finalidades distintas;

3) implementar las medidas de seguridad necesarias;

4) informar al responsable cuando ocurra una vulneración a los datos personales;

5) guardar confidencialidad; suprimir,

6) devolver o comunicar a un nuevo encargado designado por el responsable los datos personales objeto de tratamiento;

7) abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine;

8) permitir al responsable o autoridad de control inspecciones y verificaciones en sitio;

9) actualizar y conservar la documentación necesaria para el cumplimiento de sus obligaciones y

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

10) colaborar con el responsable en todo lo relativo al cumplimiento de la legislación nacional del Estado que resulte aplicable en la materia.

En caso de incumplimiento del encargado, este último asumirá la calidad de responsable desobligando a este último. (artículo 34).

Faculta a la subcontratación del servicio siempre que exista una autorización previa por escrito, específica o general del responsable, o bien, se estipule expresamente en el contrato, asumiendo el subcontratado la responsabilidad en caso de incumplimiento, conforme la legislación interna (artículo 35)

Transferencia Internacional de Datos Personales

Como regla general, en el artículo 36 (Reglas generales para las transferencias de datos personales) Capítulo V (Transferencias internacionales de datos personales) habilita las transferencias internaciones a destinatarios (territorio, sector, actividad u organización internacional) a los que se haya reconocido un nivel adecuado de protección por parte del país transferente, o que el exportador ofrezca garantías suficientes -y así lo haya acreditado- para efectuar el tratamiento en el país destinatario o que esté autorizado por la autoridad de control de Estado. Se reconocen la validez de los esquemas de autorregulación vinculante, es decir las Normas Corporativas Vinculantes, como la recientemente Resolución N°159/2018 (Normas Corporativas Vinculantes para la transferencia internacional de datos personales) dictada en Argentina por la Agencia de Acceso a la Información Pública o los mecanismos de certificación aprobado. Conforme la Resolución mencionada *ut supra*, se aprobaron los lineamientos y contenidos básicos que las empresas pueden incorporar a sus normas autorregulatorias y de esa manera, realizar transferencias internacionales hacia empresas que conformen un mismo grupo económico ubicadas en países sin legislación adecuada para la protección de datos personales. Dichos lineamientos, tendientes a que exista un rol más activo de las empresas en el control y cumplimiento normativo, indican que las normas corporativas vinculantes que pretendan alcanzar un nivel adecuado de protección de los datos personales deben ser obligatorias y exigibles tanto para la totalidad de las empresas del grupo como para los empleados, subcontratistas y terceros beneficiarios. Exige como requisito para reputarse vinculantes que existan resoluciones societarias que obliguen a cumplir con dicha norma. Asimismo, se deben incorporar los siguientes contenidos mínimos:

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

1) condiciones de licitud: engloba los principios de legitimidad del tratamiento, de finalidad y de calidad;

2) protecciones específicas por sensibilidad de la materia: incluye la prohibición del tratamiento de datos sensibles, salvo que resulte necesario por ley o con consentimiento previo del titular de los datos;

3) previsión del derecho del titular de los datos a ser excluido de los listados de publicidad directa no consentida;

4) derecho del titular de los datos a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos que le produzca efectos jurídicos perniciosos o lo afecte significativamente de forma negativa;

5) no conformación de registros de antecedentes penales y/o contravencionales y prohibición de su cesión a terceros salvo con el consentimiento expreso del titular de los datos.

Establece la responsabilidad solidaria ante el titular de los datos y la autoridad de control frente a cualquier violación de la norma de autorregulación prevista. En el marco de cooperación internacional entre autoridades de control, podrán intervenir todas las autoridades de control de las empresas importadoras y exportadoras y la obligación de la capacitación continua del personal asignado a las actividades vinculadas al tratamiento de los datos personales. (ABDELNABE VILA, 2018)

Volviendo a los Estándares y cerrando el Capítulo, prevé que la legislación nacional aplicable en la materia puede establecer expresamente límites a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

Responsabilidad Proactiva

Con el objeto de garantizar la protección de los datos, en el Capítulo VI (Medidas proactivas en el tratamiento de datos personales) se incorporaron, desde la fase de planificación de los procedimientos y sistemas de información, determinadas medidas sobre la privacidad, denominadas medidas proactivas (artículo 37). La responsabilidad proactiva supone tener en consideración la privacidad y el cumplimiento de las normativas de protección de datos desde la fase inicial del proyecto para que se diseñe e incluso se desarrolle teniendo en consideración

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

dichos requerimientos, de tal manera que la privacidad se integre en las nuevas tecnologías y prácticas empresariales directamente, desde el principio, como un componente esencial de la protección de la privacidad. Además, si se tienen en consideración estos aspectos desde el inicio, se evitará tener que redefinir los sistemas y procesos continuamente. En el artículo 38 (Privacidad por diseño y privacidad por defecto) recepta el concepto de protección de datos desde el diseño y por defecto (*Privacy by Design* -PbD-) consistente en la obligación, por parte de los responsables, de implementar desde el diseño, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones establecidas en la legislación interna. De igual manera, debe garantizar que sus programas, servicios, sistemas, plataformas informáticas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional.

Estas medidas proactivas implican la adopción de los siguientes principios:

1) Proactivo y preventivo, no correctivo: la privacidad desde el diseño suele caracterizarse por tomar medidas proactivas en lugar de reactivas, vale decir anticipar y prevenir la pérdida de privacidad de la información antes que suceda.

2) La privacidad por defecto: ofrecer el máximo grado de privacidad para asegurar que los datos personales están protegidos automáticamente en cualquier sistema informático sin necesidad de actuación por parte del cliente o proveedor, ya que está integrado en el sistema por defecto.

3) La privacidad embebida en el diseño, en la infraestructura y en los procesos de la empresa, vale decir no como un añadido sino como un componente esencial y parte integral del sistema, sin disminuir la funcionalidad.

4) Seguridad punto-a-punto – significa la protección completa del ciclo de vida de los datos, todos los datos se conservan y se destruyen de forma segura, asegurando la gestión del ciclo de vida seguro de la información, punto a punto.

5) Visibilidad y transparencia - mantenerlo abierto: garantiza a todos los interesados una verificación independiente.

6) El respeto a la privacidad del usuario por encima de todo: la privacidad desde el diseño requiere que los desarrolladores y operadores del sistema mantengan por encima de todo el interés de las personas, ofreciendo unas medidas de protección fuertes con avisos apropiados y fáciles de usar.

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

Además dichos estándares obligan al responsable a nombrar a un oficial de protección de datos personales o su equivalente en los casos establecidos en la legislación nacional y en los siguientes casos detallados en este instrumentos iberoamericano:

1) cuando sea una autoridad;

2) cuando el tratamiento de datos personales tiene por objeto una observación habitual y sistemática de la conducta del titular;

3) cuando sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, en especial si se trata de datos sensibles o si el responsable lo estima conveniente (artículo 39. Oficial de protección de datos personales) Asimismo faculta al responsable a adherirse, voluntariamente, a esquemas de autorregulación vinculante, tales como códigos deontológicos, sistemas de certificación y/o sus respectivos sellos de confianza, que tengan por objeto, entre otros, contribuir a la correcta aplicación de la legislación nacional aplicable. (artículo 40. Mecanismos de autorregulación) Y por el artículo 41 (evaluación de impacto a la protección de datos personales) obliga al responsable a realizar previamente a la implementación del tratamiento de datos personales, una evaluación del impacto a la protección de dichos datos (similar a la evaluación de impacto ambiental) siempre que exista un alto riesgo de afectación del derecho a la protección de datos personales de los titulares.

Disposiciones Finales

En virtud del Capítulo VII (Autoridades de control) obliga a los Estados Iberoamericanos a la constitución de una o más autoridades de control en materia de protección de datos personales con plena autonomía, imparcialidad e independencia en sus potestades (artículo 42. Naturaleza de las autoridades de control y supervisión). Finalmente, en los sucesivos Capítulos, se regulan el régimen de sanciones (Capítulo VIII. Reclamaciones y Sanciones) la reparación del daño (Capítulo IX. Reparación del daño) y el establecimiento de mecanismos de cooperación internacional (Capítulo X. Cooperación internacional).

CONCLUSIÓN

El alcance y masificación de la conectividad a Internet en todo el mundo, el avance de los dispositivos móviles, los blogs y las redes sociales, son fundamentales en el cambio de

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

paradigma tecnológico, económico y social. El surgimiento de las nuevas técnicas de análisis de datos masivos, comúnmente llamado "*Big data*", conjuntamente con l inteligencia artificial, directamente han venido a resignificar el concepto y el sentido de los datos y crean un entorno digital intrusivo en el que tanto los Estados como las empresas pueden llevar a cabo actividades de vigilancia, análisis, predicción y manipulación del comportamiento humano antes inimaginable.

Las revelaciones de Edward Snowden, el uso opresivo de los datos por parte de los gobiernos para identificar y arrestar a personas inocentes y el poder creciente de algoritmos que permiten la discriminación contra los menos favorecidos, son suficientes indicadores del perjuicio que el *Big Data* puede ocasionar a las sociedades democráticas basadas en los derechos humanos, fundamentalmente en la dignidad humana, la autonomía y la vida privada.

La discusión social sobre la forma en que un mundo impulsado por los datos debe configurarse apenas comienza, mientras que se sigue creando más y más datos todos los días, pero ahora los humanos no son los únicos que lo hacen. Con la llegada del Internet de las Cosas hay un mayor número de objetos y dispositivos conectados a Internet que generan datos sobre patrones de uso de los clientes y rendimiento de los productos. De ahí que, las empresas deban iniciar la transición del *Business intelligence (*Inteligencia de negocios*)*, donde se estudia un consumidor en pasado y sus consecuencias; a un *Business analytics* (Análisis de negocios), que se adelanta a las necesidades, analiza los datos en forma conjunta, establece relaciones y comparaciones entre variables para tratar de adelantarse al futuro y construye guías en tiempo real. (RAYÓN, 2015)

En consecuencia, frente a este nuevo escenario en el que predominan las tecnologías disruptivas, es particularmente necesario que los Estados adopten un marco normativo tuitivo, homogéneo, coherente y exhaustivo sobre privacidad, en especial sobre protección de datos. Y para las empresas y entidades que tratan datos de carácter personal, analizar y conocer la situación en cuanto a la adecuación a las normativas vigentes, y, sobre todo, la adopción de un sistema autorregulatorio, de control preventivo y provistos de sistemas de alerta temprana. Todas esas medidas que, además, redundan en beneficios económicos ya que evita la reconfiguración de todo el sistema o plataforma informática

En este contexto, la Red Iberoamericana de Protección de Datos Personales se muestra como una de las posibles instancias de diálogo e interacción, ya que aparte de la significativa representación de autoridades de protección de datos y de privacidad de países de la región y de

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

organismos internacionales, ha previsto en sus reuniones la participación del sector privado y de observadores académicos.

Los Estándares constituyen un primer e importante paso hacia una mayor armonización de la legislación a nivel regional. Se presentan como un modelo normativo flexible que responde a las necesidades y exigencias nacionales e internacionales en la materia y que garantizan un nivel adecuado de protección de los datos personales sin establecer barreras a la libre circulación y a las actividades comerciales en la región. Las legislaciones de los Estados Iberoamericanos deben fijar medidas que promuevan el cumplimiento de la legislación de protección de datos, entre las que destaca, la obligación de cada Estado Iberoamericano de establecer una o más autoridades de control en materia de protección de datos personales con plena autonomía y adoptar mecanismos de cooperación internacional.

Recordando las palabras del visionario escritor George Orwell, en su libro 1984: *"Con el desarrollo de la televisión y el adelanto técnico que hizo posible recibir y transmitir simultáneamente en el mismo aparato, terminó la vida privada".* (ORWELL, 1984, p. 221)

La idea es que no termine la vida privada sino que se reconfigure, se adapte y actualice la legislación para asegurar el derecho a la intimidad, a la dignidad y al honor conforme la economía digital vigente en este siglo XXI, para lo cual, en primer lugar hay que reconocer y comprender el funcionamiento de este fenómeno para después regularlo técnica y jurídicamente.

THE PROTECTION OF PERSONAL DATA IN THE DIGITAL ENVIRONMENT. DATA PROTECTION STANDARDS FOR IBERO-AMERICAN STATES

Abstract
The noticeable increase of Internet and social networks has generated a scenario in which more and more personal data are collected, stored and analyzed, generating even new data from that treatment from which the individual in which the information originated totally unaware The data is beginning to be used and reused for the most diverse purposes, many of which can be harmful to the owner. Therefore, it is necessary to update the meaning of the right to privacy in a digital economy, in which the protection of personal data has become a fundamental part, as well as providing an integral and tuitive legal framework. For this purpose, the objective of this paper is to analyze the current meaning of the right to privacy in a digital economy and the guidelines of legal regulation established in the Data Protection Standards in the Ibero-American States. In order to comply with this objective, the methodology was based, first, on the delimitation and updating of the conceptual framework to later analyze the different principles adopted in the Data Protection Standards in the Ibero-American States.

Keywords: Personal Data - Digital Environment - Law - Protection Standards - Ibero-American.

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

REFERENCIAS BIBLIOGRÁFICAS

ABDELNABE VILA, Carolina. "Argentina se adapta a la normativa europea, mientras espera la sanción de la nueva Ley de Protección de Datos Personales" **Abogados.com.** 13 de febrero de 2019. Recuperado el 13 de febrero de 209, de http://abogados.com.ar/...-la-normativa-europea-mientras-espera-la-sancion-de-la-nueva-ley-de-proteccion-de-datos-personales/22921

_____. "Un paso más hacia la autorregulación corporativa en materia de datos personales" **Abogados.com.** 17 de diciembre de 2018. Recuperado el 17 de diciembre de 208, de http://abogados.com.ar/un-paso-mas-hacia-la-autorregulacion-corporativa-en-materia-de-datos-personales/22698

ASOCIACIÓN POR LOS DERECHOS CIVILES. **El sistema de protección de datos personales en América Latina: Oportunidades y desafíos para los derechos humanos.** Buenos Aires, Argentina: ADC, 2017, 40 p.

ARGENTINA. AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA. *Resolución 4/2019. Anexo Criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley Nº 25.326*. Boletín Oficial de la República Argentina. Recuperado el 8 de febrero de 2019, de https://www.boletinoficial.gob.ar/#!DetalleNorma/200224/20190116

_____ Códigos (2014) *Código Civil y Comercial de la Nación.* 1° Edición. Ciudad Autónoma de Buenos Aires, Argentina: Infojus, 2014, 512 p.

BBC MUNDO. "La polémica por la manipulación emocional de Facebook", **BBC Mundo**, 30 de junio de 2014. Recuperado el 3 de febrero de 2018, de http://www.bbc.com/mundo/noticias/2014/06/140630_tecnologia_facebook_experimento_emociones_criticas_lv.

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE. **Datos, algoritmos y políticas. La redefinición del mundo digital.** Santiago, Chile: CEPAL, 2018, 186 p.

ESPAÑA. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **Código de Buenas Prácticas en Protección de Datos Personales Para Proyectos de Big Data**. España: AGPD. 2017, 40 p.

_____ TRIBUNAL CONSTITUCIONAL. Sentencia 58/2018, de 4 de junio de 2018. *Recurso de amparo 2096.2016*. BOE, núm.164, p. 68409 – 68433

HUMAN RIGHTS COUNCIL. "The right to privacy in the digital age". 3 august 2018. **A/HRC/39/29**

LICEDA, Ernesto. "La identidad digital" **Revista Anales**, La Plata, Argentina, n. 41, 2011, p. 296-304

MARTÍNEZ, Adriana; PORCELLI, Adriana. "Consumo (In) Sostenible: Nuevos Desafíos frente a la Obsolescencia Programada como Compromiso con el Ambiente y la Sustentabilidad" **Ambiente y Sostenibilidad.** Revista del Doctorado Interinstitucional en Ciencias Ambientales, 2016, Bogotá, Colombia, vol. 6, p. 105-135.

MENDOZA, Miguel Ángel. "El derecho a la privacidad en la era digital" **welivesegurity**. 2 de marzo de 2017. Recuperado el 25 de enero de 2018, de https://www.welivesecurity.com/la-es/2017/03/02/derecho-a-la-privacidad-era-digital/

MORELLO, Augusto. **Constitución y Proceso**. Buenos Aires, Argentina: Abeledo Perrot. 1998, 448 p.

ORGANIZACIÓN DE LAS NACIONES UNIDAS- ONU. ASAMBLEA GENERAL. Resolución aprobada por la Asamblea General el 19 de diciembre de 2016. 71/199 *El derecho a la privacidad en la era digital*. **A/RES/71/199**

vol. 12, nº. 02, Rio de Janeiro, 2019. pp. 465-497
DOI: 10.12957/rqi.2019.40175

____ CONSEJO DE DERECHOS HUMANOS. Resolución aprobada por la Asamblea General el 24 de marzo de 2015, N° 28/L.27. *El derecho a la privacidad en la era digital*. **A/HRC/28/L.27**

ORWELL, George. **1984.** Sexta Edición. Barcelona, España: Ediciones Destino S.A., 1984, 318 p.

RANKING DIGITAL RIGHTS. **2018 Corporate Accountability Index**. New York, Estados Unidos: New America's Open Technology Institute, 2018, 145 p.

RAYÓN, Álex. "Por qué hablamos del Business Analytics y no solo del Business Intelligence". **DeustoData.** 6 de diciembre de 2015. Recuperado el 12 de diciembre de 2018, de https://blogs.deusto.es/bigdata/por-que-hablamos-del-business-analytics-y-no-solo-de-business-intelligence/

RED IBEROAMERICANA DE DATOS PERSONALES. **Estándares de Protección de Datos Personales para los Estados Iberoamericanos**. Colombia: RIPD, 2017, 34 p.

SIBILIA, Paula. **La intimidad como espectáculo**. Buenos Aires, Argentina: Fondo de Cultura Económica, 2008, 325 p.

UNITED NATIONS HUMAN RIGHTS. "Too much surveillance: Respect civil liberties and stop playing 'fear card', says UN expert". **News and Events**. 8 march, 2017. Recuperado el 3 de febrero de 2019, de https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21321&LangID=E

Trabalho recebido em 14 de fevereiro e 2019
Aceito em 12 de março de 2019