bioeticar
Asociación Civil

>> Haciendo lazos

La necesidad de ejercer una ciudadanía digital responsable[1]

Mg. Gricelda Moreira*

Las legislaciones van ajustándose a los nuevos adelantos, pero es necesario que los ciudadanos aprendamos a tomar decisiones digitales responsables.

En materia de salud, los datos digitales pueden surgir de registros médicos electrónicos e imágenes, aunque también de datos farmacológicos, ambientales y hábitos de los pacientes, entre otros. Así, *Big Data* permitiría mejorar la capacidad de respuesta del sistema de salud pública, incrementar la detección temprana de enfermedades y reducir los tiempos de investigación médica, o bien, avanzar hacia una medicina personalizada utilizando los datos de pacientes.

En el campo sanitario, la difusión y el cruce de información en la Web entraña riesgos para los derechos fundamentales de las personas en tanto los datos sensibles almacenados pueden usarse para mejorar la atención de los pacientes, direccionar publicidad o incluso discriminar a personas con determinadas patologías. Google, utilizado por el 68% de estadounidenses y el 90% de europeos, reconoce que una de cada cinco búsquedas en línea se vincula con la salud, lo que abre las puertas para que compañías de *marketing* o empresas dedicadas al almacenamiento de datos puedan recoger información sensible para luego comercializarla.

Este nuevo contexto requiere ser analizado críticamente para así proponer medidas consistentes para la protección de datos. Hasta el momento, la anonimización permitió cumplir con las normas de protección de los datos personales, es decir que al ser estos anonimizados, dejan de contener información sensible, pero así quedan por afuera de la protección legal. El problema es que gracias al uso de técnicas de ingeniería informática se pueden cruzar datos e identificar a quien pertenecen, volviendo obsoletas las medidas de resguardo del anonimato. (Moreira, G., Ruffa A. et al, 2020)

---

[1] Articulo completo en Moreira, G. (2021) *La propagación digital y la muerte del anonimato.* Disponible https://www.academia.edu/45216729/La_propagaci%C3%B3n_digital_y_la_muerte_del_anonimato?email_work_card=view-paper

Aunque suele confundirse con la confidencialidad, en rigor el anonimato es la condición de anónimo, concepto procedente del griego que puede traducirse como “sin nombre”. Sin registro de datos que identifiquen a la persona, no hay responsabilidad en proteger ninguna confidencialidad puesto que no es posible establecer un vínculo entre unos datos y la identidad de una persona.

Internet es el gran medio para transportar información, tanto personal como financiera, pero navegar en la red no es una actividad anónima. (Brizzolis, 2020) Nombre, correo e electrónico, ubicación, interacciones, preferencias, son los datos de usuarios que recopilan las aplicaciones más utilizadas. Cuando se aceptan los términos y condiciones, se da acceso a las compañías a que obtengan y guarden cierta cantidad de información que luego estas empresas emplean para prestar sus servicios.[2] Datos estructurados, semiestructurados y no estructurados, tienen el potencial de ser extraídos para aportar información de cualquier tipo, sea financiera, económica, social, geoespacial, meteorológica, de planificación de una ciudad, de publicidad.[3]

La idea de que la tecnología es infalible nos hace perder de vista que quienes hacen la recolección de datos realizan un corte sesgado, que los datos pueden estar desactualizados, pueden ser erróneos, pudiendo provocar una discriminación algorítmica, por ejemplo, hacer aparecer a una persona en una base de datos de deudores cuando ya pagó su deuda, lo que le imposibilita sacar un préstamo o incluso ingresar a un nuevo trabajo. “[…] pueden presentar problemas de insuficiencia, errores, y exceso o déficit de representación de ciertos grupos de la sociedad, todo lo cual podría redundar en una decisión algorítmica equivocada”. (Snowden, 2017) Por tanto, si bien los Estados elaboran normativas, la responsabilidad también es nuestra, en cada clic brindamos información que genera algoritmos[4] que pueden inducirnos a tomar ciertas decisiones en la vida, poniendo entre paréntesis nuestra libertad de elección. Según Harari,[5] la ciencia converge en un dogma universal que afirma que los organismos, incluido el ser humano, no son más que algoritmos y que la vida es procesamiento de datos.

---

[2] Ver https://www.infobae.com/america/tecno/2020/10/30/cuales-son-las-aplicaciones-que-tienen-mas-informacion-de-sus-usuarios/

[3] La vulnerabilidad no deja exentos a los gobiernos mundiales de filtraciones. Solo a modo de ejemplo, el CIPER Chile (centro de investigaciones periodísticas) detectó en 2016 que era posible acceder a datos sensibles contenidos en carpetas compartidas en las redes del Ministerio de Salud de ese país, fisura que dejó alrededor de 3.000.000 de archivos expuestos. Otro caso, fechado en 2019, fue el de la información perteneciente a 20.000.000 de ecuatorianos, desde sus números de documentos, correos electrónicos, número de celulares, domicilios, lugar de trabajo. (Ver https://www.ciperchile.cl/2016/03/05/ y https://medium.com/saturdays-ai/los-desaf%C3%ADos-%C3%A9ticos-de-la-ciencia-de-datos-25ce771d892e)

[4] Algoritmo: conjunto de instrucciones o reglas definidas y no ambiguas, ordenadas y finitas que permite solucionar un problema, realizar un cómputo, procesar datos y llevar a cabo otras tareas y actividades.

[5] Yuval Noah Harari (1976), historiador y escritor israelí, profesor de la universidad hebrea de Israel.

(Harari, 2016) Ello puede afectar los comportamientos y decisiones individuales, volverse una sofisticada manipulación de las masas.

Nuestra información está por todas partes, más allá de nuestro consentimiento: “Ahora mismo, seas quien seas, estés donde estés, en términos corpóreos y físicos, te encuentras además por todas partes, estás en circulación […]. Nuestros datos deambulan a lo largo y a lo ancho” (Snowden, 2017).

¿Qué medidas adoptaron los Estados para asegurar la privacidad y transparencia en la recolección de datos personales?

La defensa de la privacidad y la necesidad de ser regulada a través del derecho no es nueva. A nivel internacional existen declaraciones –como la Declaración Universal de los Derechos Humanos (1948)–, convenciones –como el Pacto Internacional de Derechos Humanos y Políticos (1966); Convención Americana de Derechos Humanos,[6] Convención Americana sobre Derechos Humanos (Pacto de San José), Costa Rica 1969–.[7] Asimismo, la Convención Europea de Derechos Humanos, en su artículo 8 expresa que: “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”.[8]

La privacidad, es un derecho humano que encuentra su fundamento en instrumentos internacionales y nacionales. El derecho se ocupa de elaborar normas que la protejan en el ciberespacio, habida cuenta de los efectos en la vida cotidiana de los ciudadanos.

El Reglamento General de Protección de Datos –RGPD 2018 de la Unión Europea– regula específicamente la creación de perfiles y lo define como el análisis o la predicción de aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos, y establece que las personas tendrán derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos sobre él o le afecte significativamente de modo similar.[9]

Para el manejo de datos personales se plantean seis principios básicos: ser tratados de forma lícita, leal y transparente, ser recolectados con fines determinados, explícitos y legítimos, limitarse a lo necesario dependiendo del uso, deben ser exactos y estar siempre actualizados,

---

[6] Disponible en http://www.ohchr.org/S P/ProfessionalInterest/ Pages/CCPR.aspx 41

[7] Disponible en https://www.oas.org/dil/esp/tratados _B-32_Convencion_ Americana_sobre_Derechos_Humanos.pdf

[8] Disponible en https://www.derechoshumanos.net/Convenio-Europeo-de-Derechos-Humanos-CEDH/articulo8CEDH.htm

[9] Disponible en https://revistas.uam.es/revistajuridica/article/view/10227

mantenerse de forma tal que se permita la identificación de los interesados durante no más tiempo del necesario y deben manipularse de tal manera que se garantice su seguridad. Sin entrar en detalles específicos del Reglamento, uno de los elementos esenciales es que en él se establece el consentimiento como base de la gestión de datos personales en casi todos los casos. Esto implica que, además de los temas atinentes a la seguridad y a la legalidad, quienes recolecten y gestionen los datos deberán asegurarse siempre de haber informado a los propietarios de estos datos y obtener su consentimiento tantas veces como se requiera si la finalidad del uso que se le dará a sus datos cambia.

Por su parte, el Supervisor Europeo de Protección de Datos (2015) propone combinar la información, la dignidad y la tecnología para una ética digital. A través del dictamen N°.4/2015, define: "La dignidad humana es inviolable. Ha de respetarse y protegerse".[10]

En nuestra legislación, en la Constitución Nacional[11] se establecen las garantías que permiten a toda persona interesada acceder al conocimiento de los datos que consten en registros o bancos de datos públicos o privados destinados a proveer informes, exigir su supresión, rectificación, confidencialidad o actualización, en caso de falsedad.

Por su parte, la Ley 25.326/2000[12] sobre la protección de los datos personales, refiere a la legitimación activa –quién puede reclamar– y a la legitimación pasiva –a quién se le reclama.[13] Esta busca proteger el derecho a la intimidad y privacidad de los datos sensibles –origen racial y étnico, convicciones religiosas, filosóficas o morales, afiliación sindical, opiniones políticas e información referente a la salud o a la vida sexual– al permitir a las personas acceder al registro de datos que posee el organismo correspondiente, actualizar, rectificar o corregir información errónea y preservar la confidencialidad para que la misma no sea expuesta públicamente a terceros, así como suprimir datos que afecten la intimidad o que puedan usarse con fines discriminatorios.[14] En igual vía se establece que el tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento[15] libre, expreso e

[10] Ver European Data Protection Supervisor, 2015 https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_es.pdf
[11] Constitución de la Nación Argentina, Ley 24.430 (apdo. 3° del art. 43 de la CN de 1994).
[12] Disponible en: https://www.oas.org/juridico/pdfs/arg_ley25326.pdf
[13] Excepciones a dichas garantías: 1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obliga. Ver https://www.oas.org/juridico/pdfs/arg_ley25326.pdf
[14] Ver https://www.oas.org/juridico/pdfs/arg_ley25326.pdf
[15] Ley 21.526, artículo 5° (consentimiento). 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por

informado, el que deberá constar por escrito o por otro medio que permita se le equipare, de acuerdo con las circunstancias. El consentimiento dado[16] para el tratamiento de datos personales puede ser revocado en cualquier tiempo y dicha revocación no tiene efectos retroactivos.[17]

En la práctica, los usuarios no suelen tomarse el tiempo para leer y comprender todos los términos y condiciones de uso, para entender exactamente a qué acceden, lo cual es lógico, debido a que es materialmente imposible. Según un informe de Visual Capitalist[18] se necesitarían 250 horas para leer los acuerdos de todos los servicios que se utilizan en celulares o computadoras, a lo que se suma la dificultad para comprender muchos de estos textos que no están necesariamente escritos en un lenguaje sencillo.

La privacidad en Internet implica considerar todos los aspectos que se plantean, desde el tratamiento de los datos personales con fines publicitarios hasta la vigilancia electrónica, así como la interrelación que este derecho tiene con otros derechos humanos, tales como el derecho a la libertad de expresión. (Soto, 2017)

Hasta aquí algunos de los principios rectores esgrimidos en el marco normativo sobre el tratamiento de los datos personales. Más allá, es importante que las autoridades concienticen a la ciudadanía sobre la protección de datos y la importancia del consentimiento informado y accesible.

---

escrito, o por otro medio que permita se le equipare, de acuerdo con las circunstancias. El referido consentimiento prestado con otras declaraciones deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley. 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm, recuperado 5 de nov 2020.

[16] Con las TICs surgieron algunos neologismos, como el de *Habeas Data*: *habeas* proviene del latín, es la segunda persona singular del presente subjuntivo del verbo *habēre* (“tener”) que significa “aquí tengas en posesión”, como una de las acciones del verbo, y *data* es el acusativo plural de *datum*, “lo que se da”, información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho.(DRAE) Dicha información personal en ocasiones es requisito o condición para acceder a un servicio y se proporciona de manera voluntaria, a veces involuntaria, quedando disponible en sistemas o soportes electrónicos.

[17] Ver reglamentación del Decreto 1.558/016 6 en el artículo 5 disponible en: http://www.infoleg.gov.ar/infolegInternet/verNorma.do?id=70368 recuperado 5 de nov 2020

[18] Ver https://www.infobae.com/america/tecno/2020/10/30/cuales-son-las-aplicaciones-que-tienen-mas-informacion-de-sus-usuarios/ recuperado 3 de nov 2020

De nuevo, el Supervisor Europeo de Protección de Datos (2015) expresa en su artículo 1° que "[…] en el entorno digital actual, no basta con respetar la ley, sino que es preciso tener en cuenta la dimensión ética del tratamiento de datos", es decir que el debate trasciende la vertiente legal. Se trata de un cambio de paradigma que requiere no solo de legislaciones internacionales, regionales y nacionales que resguarden el derecho humano a la intimidad, sino también generar ciudadanos digitales responsables. Es preciso que los propios usuarios tomen conciencia de la vulnerabilidad a la que quedan expuestos y que se puedan adoptar medidas para hacer un uso responsable de la tecnología.

Jorge Balladares,[19] en su escrito *Una ética digital para las nuevas generaciones digitales*, refiere a la necesidad de fomentar la construcción de referentes y comportamientos digitales, que contribuya a los deberes y derechos de las nuevas generaciones. La ética permite discernir y lograr una relación armónica entre las personas y la tecnología. (Balladares, 2017).

Noviembre, 2022

** Licenciada en psicología (UBA), Psicoanalista (EFBA), Magíster en Bioética (FLACSO), Doctoranda en Ciencias Sociales (UBA), Diplomada en Psicología en Reproducción Asistida IUNIR- SAMER de la Sociedad Argentina de Medicina Reproductiva. Actualmente se desempeña como Presidenta de Bioeticar Asociación Civil, Subdirectora del Centro de Bioética de la Universidad ISALUD y es Miembro de la International Association of Bioethics (IAB). Sus temas de investigación son los dilemas éticos de la reproducción tecno-mediada y la vitrificación de óvulos por causas no terapéuticas.*

BIBLIOGRAFÍA

Balladares, J. (2017). *Una ética digital para las nuevas generaciones digitales* 557 Revista Puce. ISSN: 2528-8156. NÚM.104., PP. 543-563.

Brizzolis, F. (2020). *Anonimato y privacidad práctica en internet*. Disponible en: https://derechodelared.com/wp-content/uploads/2020/06/Anonimato.pdf, recuperado el 5 de noviembre de 2020.

Harari, Y. (2016). *Homo Deus*. Debate. Buenos Aires

Moreira, G., Ruffa, A., Soifer G. (2020). *Los desafíos en torno a la privacidad y la vigilancia en tiempos de COVID-19,* en Anuario de Bioética y Derechos Humanos del Instituto Internacional de Derechos Humanos (IIDH) Capítulo para las Américas. Compilado por

[19] Jorge Balladares actualmente trabaja en la Universidad Andina Simón Bolívar en Quito, Ecuador, realiza investigación en TIC para la Educación, Tecnología Educativa, Ética, Filosofía de la Ciencia y Filosofía Social y Política.

Eduardo Luis Tinant. - 1a ed. compendiada. - Ciudad Autónoma de Buenos Aires. 2020. Libro digital, Amazon Kindle Archivo Digital: descarga y online ISBN 978-987-86-7013-3, pág. 62

Snowden E. (2017). *La gestión de los datos*. Disponible https://www.cels.org.ar/web/wp-content/uploads /2017/06/Vigilancia-y-democracia_INCLO.pdf recuperado 4 de nov 2020

Soto, Y. (2017). *Datos masivos con privacidad y no contra privacidad* en Dossier monográfico XII congreso mundial Datos masivos con privacidad y no contra privacidad Big Data. Disponible en http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872017000200008, recuperado el 4 de noviembre de 2020.

¿Cómo citar?

Moreira, G.,2022 La necesidad de ejercer una ciudadanía digital responsable. *Boletín Bioeticar Asociación Civil*, vol. II, N°6, noviembre 2022, ISSN 2953-3775 https://www.bioeticar.com.ar/boletin6.html