El uso de información en el área de la salud[*]

The Use of Data in the Health System

María Ángeles Salazar-Arenas[**]
Rubí Viveros-Contreras[***]

[*] Esta publicación fue realizada con el apoyo del Doctorado en Ciencias Biomédicas del Centro de Investigaciones Biomédicas de la Universidad Veracruzana, campus Xalapa, y con el apoyo del Consejo Nacional de Ciencia y Tecnología (CONACYT) (Beca 691229).

[**] Maestra en Nutrición Clínica por el Instituto Nacional de Salud Pública en colaboración con el Instituto Nacional de Perinatología, Ciudad de México. Doctoranda en Ciencias Biomédicas en el Centro de Investigaciones Biomédicas de la Universidad Veracruzana, México. Correo electrónico: angelesalazar90@gmail.com. ORCID: 0000-0002-9944-4271.

[***] Doctora en Ciencias por la Escuela Nacional de Ciencias Biológicas del Instituto Politécnico Nacional. Profesora-Investigadora en el Centro de Investigaciones Biomédicas de la Universidad Veracruzana, México. Miembro del SNI (Nivel I). Correo electrónico: ruviveros@uv.com. ORCID: 0000-0003-3126-6664.

Resumen
El uso de información en salud se ha incrementado con la digitalización de los expedientes clínicos y el análisis de grandes volúmenes de información recolectada a través de las tecnologías de la información y comunicación, lo que ha permitido contribuir en una mejora en la atención médica y apoyar la investigación en salud. Sin embargo, el tratamiento indiscriminado de datos personales junto con las nuevas técnicas de inteligencia artificial puede aumentar la vulnerabilidad de los usuarios de salud y poner en riesgo su autonomía, confidencialidad y derecho a la privacidad. El ejercicio profesional en la práctica clínica e investigación en salud requiere del resguardo responsable de los datos, de tomar medidas estrictas de seguridad controlando y limitando el acceso a la información, además de conocer y cumplir la regulación en materia de protección de datos personales y de solicitar consentimientos informados válidos que permitan mantener el Código de Ética Médica.

Palabras clave: Autonomía, confidencialidad, datos personales, privacidad, vulnerabilidad.

Abstract
The use of data in health has increased due to the digitalization of clinical records and the analysis of big amount of data collected through information and communication technologies, which has allowed to improve the medical care and support health research. However, the indiscriminate use of personal data combine with new artificial intelligence techniques may increase the vulnerability of health users and their autonomy, confidentiality, and right of privacy. Professional practice in clinics and health research requires the responsible custody of the health user´s data, stablishing strict security measures, controlling and regulating the access to information, in addition of being acquainted of and exercising the regulations of personal data protection besides requesting valid informed consents that allow to maintain the Code of Medical Ethics.

Key words: Autonomy, confidentiality, personal data, privacy, vulnerability.

Introducción

El uso de información en salud es una práctica habitual que se ha incrementado con el avance en las tecnologías de la información y comunicación, lo que a su vez ha permitido el almacenamiento y análisis de grandes cantidades de datos, así como de la digitalización de la información médica (Li, Zou, Liu y Chen, 2011; Malgieri y Niklas, 2020).

Ahora no solo se cuenta con los registros de salud electrónicos para la investigación, sino que se complementa con información proveniente de Internet y aplicaciones de salud, lo que facilita la generación de conocimiento y mejora los servicios de salud (Kaplan, 2014). No obstante, el tratamiento de datos de salud sin regulación representa un riesgo para la privacidad, seguridad y autonomía de las personas, convirtiéndose en un problema ético y legal (Li *et al*., 2011; Rumbold y Pierscionek, 2017).

Todos los días se generan, recopilan y procesan grandes conjuntos de datos que tienen un potencial de uso indeterminado (Vayena y Blasimme, 2017), poniendo en peligro la privacidad de los usuarios, cuestión que obliga a los proveedores de servicios de salud e investigadores afines a esta área de conocimiento a conocer las medidas de seguridad para la información así como el marco jurídico para la protección de datos personales.

La información personal

Los datos personales son cualquier información que permite identificar a una persona a través de su descripción, lugar de residencia, trayectoria académica y laboral (Gómez Sánchez, 2020; Mendoza Enríquez, 2018).

Los datos personales engloban a los datos personales sensibles, que se relacionan con la esfera más íntima de una persona como lo son el origen étnico, el estado de salud, la información genética, las creencias religiosas e ideología, las preferencias sexuales y la información financiera. La utilización de datos sensibles puede poner en riesgo de

discriminación y marginación a las personas (Gómez Sánchez, 2020; Mendoza Enríquez, 2018).

Los datos personales tienen un valor económico, que no radica en la información aislada sino en su tratamiento asociado con otros datos y la finalidad con la que se analicen, es decir, conjuntando diversos datos sobre una persona puede generarse su perfil para diferentes propósitos (Mendoza Enríquez, 2018).

El alcance de la información

Debido a los avances tecnológicos, en la actualidad gran parte de la población tiene acceso a información de diversa índole, al mismo tiempo que, de forma voluntaria e involuntaria, participa en la generación de datos sobre preferencias, ideas y otras características personales que alimentan grandes repositorios de datos. Cuando las personas utilizan dispositivos electrónicos cualquier interacción entre usuarios (chats, correos, audios, etcétera), o directamente con los mismos dispositivos (consulta de aplicaciones en el celular o grabaciones de seguridad, entre otros), permite el registro de datos que posteriormente se tratan con diferentes fines como la investigación, mercadotecnia, finanzas y política (Fonseca, 2017).

Todos los patrones, conductas, registros de datos personales y búsquedas pueden verse almacenados, analizados y comparados con otros datos (Alfaro, 2012). Este registro de información de salud ha promovido avances en el diagnóstico, prevención y tratamiento de enfermedades, así como para realizar estudios epidemiológicos a gran escala y de bajo costo (Mittelstadt y Floridi, 2016; Rumbold y Pierscionek, 2017).

La nube consiste en un conjunto de servicios y plataformas de almacenamiento de datos en Internet (El Kettani, Housban, Serhier y Othmani, 2018). Su capacidad es prácticamente ilimitada y contiene datos de todas las características posibles (Mittelstadt y Floridi, 2016). Las empresas, organizaciones e instituciones del área de la salud pueden contratar estos repositorios para almacenar su información y compartirla con otros para intereses diversos en salud (El Kettani *et al*., 2018). El

conjunto de datos estructurados y no estructurados que se recopilan en la nube reciben el nombre de Big Data (Fonseca, 2017). Para el análisis de Big Data se emplean técnicas de Inteligencia Artificial, que simulan los procesos de inteligencia humana permitiendo obtener conclusiones y predicciones de los datos de interés (Martínez-García, Dalgo-Flores, Herrera-López, Analuisa-Jiménez, Velasco-Acurio, 2019). La nube y Big Data pueden considerarse una forma de negocio de venta tanto de almacenamiento como tratamiento de datos (Mittelstadt y Floridi, 2016). Ejemplo de la comercialización de la información son los famosos casos en la corte de Sorrel y Source, en el que farmacias minoristas vendieron la información de recetas de prescripción médica anonimizadas a empresas de minería de datos, que posteriormente ponían a la venta los informes resultantes a las compañías farmacológicas, y éstas últimas adecuaban su promoción y costo de fármacos. En ambos casos, los tribunales permitieron a las empresas de minería de datos continuar con el ejercicio, ya que al utilizar información anonimizada no violaban la confidencialidad de médicos y usuarios (Geri y Lafferrière, 2014; Kaplan, 2015).

Digitalización de la información médica

Uno de los grandes progresos en el área de la salud fue la digitalización de la información. Los historiales médicos con datos demográficos, diagnósticos, notas de seguimiento, tratamientos, pruebas bioquímicas, estudios de imagen quedan registrados de manera electrónica (Li *et al*., 2011). Estos registros de salud tienen valor y utilidad en el campo administrativo, legal, financiero, de investigación, educación y documental (Sugiarti y Prodi III, 2020).

El sistema de salud electrónico facilita el acceso a la información mejorando la calidad de atención, la coordinación entre especialistas y la toma de decisiones, al mismo tiempo que se reducen los errores médicos, los costos y el tiempo de servicio (El Kettani *et al*., 2018; Li *et al*., 2011). El análisis de datos históricos como la duración de estancia hospitalaria, características de los pacientes hospitalizados y en área

crítica, las cirugías más recurridas, las principales complicaciones en un grupo de pacientes específico, entre otros ejemplos, puede facilitar la predicción de resultados clínicos que sirvan de base para mejorar la atención en salud (Boilson, Staines, Connolly, Connolly y Davis, 2018).

Paralelamente, el uso generalizado de los expedientes representa un riesgo de exposición para los usuarios, por lo que las medidas de seguridad y privacidad deben ser prioritarias, reglamentando quién puede tener acceso a los archivos médicos, bajo qué condiciones y cuál es considerado el uso inapropiado de la información (Li *et al*., 2011).

Algo común en el área médica son las prácticas de estudiantes a los cuales se les permite el acceso a expedientes, incluso muchas veces se les pide reporten casos clínicos con la finalidad de fomentar el aprendizaje. Por lo que parte de la formación de estudiantes debe incluir capacitaciones en tema de propiedad y protección de datos, e implementar la firma de cartas de confidencialidad para la información a la que se les dará acceso (Bondre, Pathare y Naslund, 2021).

En última instancia, el usuario de salud tiene la autoridad de especificar en qué condiciones debe compartirse su información. Los derechos de los usuarios están directamente relacionados con las obligaciones del personal de salud, quienes deben asegurar la confidencialidad de la información compartida (Sugiarti y Prodi III, 2020).

El sistema Adhaar de la India es evidencia del riesgo latente de exponer la información de salud. Este sistema consiste en una clave de salud única asociado al número de identidad de 12 dígitos para cada habitante. Bajo esta clave se registran datos demográficos, biométricos, de salud, para la entrega de beneficios, subsidios, pensiones, está vinculado a cuentas bancarias y de telefonía móvil. Por lo que ahora representa la forma más usada para la autentificación y, por consiguiente, su uso no autorizado podría permitir la identificación de los habitantes indios junto con la exposición de toda su información (Bondre *et al*., 2021).

En el caso de México, el Sistema Nacional de Salud se encuentra fragmentado por la condición laboral y es muy heterogéneo (Medina-Gómez y López-Arellano, 2019). Principalmente se pueden hablar de dos sectores, el público y privado, aunque el sector público está a su vez dividido entre las personas asalariadas que cuentan con seguridad social y aquellos sin empleo formal, que no tienen seguro, bajo la atención

de la Secretaria de Salud (Díaz de León Castañeda y Góngora Ortega, 2020). Esta fragmentación dificulta la cobertura total de salud de la población mexicana, así como la utilización por parte de todos los niveles de salud de las tecnologías de la información y comunicación, causado entre otras cuestiones por la falta de infraestructura, de recursos económicos, materiales y humanos, así como la dificultad para llevar estas tecnologías a poblaciones lejanas y con pocos habitantes. El hecho de que algunas organizaciones o clínicas de salud no cuenten con sistemas electrónicos, impide la correcta supervisión de sus actividades, repercutiendo en su eficiencia y calidad, además de perjudicar principalmente en un trato justo a grupos con bajos recursos, sin empleo formal, población indígena o de comunidades rurales (Díaz de León Castañeda y Góngora Ortega, 2020; Gutiérrez *et al*., 2019). La falta de alcance de las tecnologías de información y comunicación en México, adicionado a la injusta repartición de equipamiento y recursos, se ha reflejado en el aumento de la demanda de servicios del sector privado de poblaciones sin empleo formal, indígena y de bajos recursos aumentando su vulnerabilidad (Flores-Hernández *et al*., 2019).

Problemas con el uso de información de salud

Con la implementación de la nube, Big Data y las técnicas de inteligencia artificial, el potencial de utilidad de la información médica es ilimitado, al mismo tiempo que los temas éticos de propiedad, privacidad, confidencialidad, vulnerabilidad y protección de datos deben atenderse (Mittelstadt y Floridi, 2016).

Con la extracción de datos de diversos medios surgen desafíos para respetar la autonomía de la población (Kaplan, 2014). Una de las formas de salvaguardar la autonomía es informar sobre el uso de datos mediante un consentimiento informado para que cada persona pueda acceder o negarse a proporcionarlos (Howe Iii y Elenberg, 2020). A pesar de esto, cuando se utiliza información pública no se suele solicitar el consentimiento, ya que se utilizan técnicas para proteger la identidad de las personas, lo que restringe la libre elección mientras que la ano-

nimización no impide que los resultados afecten de forma indirecta a ciertos grupos (Howe Iii y Elenberg, 2020; Kaplan, 2014; Mittelstadt y Floridi, 2016).

La confidencialidad está relacionada con el derecho a la privacidad, a la autonomía y a las normas de la práctica profesional en salud. Mediante el juramento hipocrático, los médicos se comprometen a mantener la confidencialidad de los usuarios de la salud, excepto cuando la protección del interés público o de otras personas requiera invalidarla. El derecho a la confidencialidad también se establece como normativa en el Código Internacional de Ética Médica de la Asociación Médica Mundial (AMM, por sus siglas en inglés) y la Declaración de Helsinki. La confidencialidad puede comprometerse al recopilar, documentar y divulgar la información en temas de salud, especialmente cuando se trabaja en bases de datos en la nube que podrían combinarse con otras fuentes de información (Kaplan, 2014).

El riesgo de divulgación involuntaria aumenta con las crecientes brechas en los sistemas de seguridad, como en los casos de robo de cintas de grabación y portátiles con la información de usuarios o intrusiones en los sistemas web (Karasneh, Al-Azzam, Alzoubi, Hawamdeh y Muflih, 2019). Todas las personas están expuestas a la violación de su privacidad que, en caso de tratarse de información sensible, las pone en riesgo de discriminación, marginación, estigma y aumento de los costos de la atención médica (Price y Cohen, 2019).

Así mismo el uso de Big Data implica desigualdades entre quienes proporcionan los datos y los custodios de la información, que normalmente son quienes la venden obteniendo grandes beneficios sin considerar las consecuencias para los primeros (Mittelstadt y Floridi, 2016). Es así que con el libre acceso a los datos públicos, nuevos grupos vulnerables emergen debido a la reidentificación y violaciones a la privacidad (Howe Iii y Elenberg, 2020; Malgieri y Niklas, 2020).

En este contexto, las diferentes condiciones económicas, históricas y sociales impactan en el ejercicio de los derechos. A lo largo de la historia, se ha tomado ventaja de grupos de mayor vulnerabilidad, que han sido explotados con fines de investigación para ventaja de otros, por lo que ahora existen lineamientos éticos, como la Declaración de Helsinki y el Código de Núremberg, que velan por la dignidad humana y el cum-

plimiento de sus derechos priorizando los beneficios sobre los riesgos (Malgieri y Niklas, 2020).

Por lo tanto, la reglamentación en investigación médica tiene por objeto proteger a aquellos que, por definición, son más vulnerables (Rumbold y Pierscionek, 2017). En el área de investigación en salud todo protocolo debe ser revisado y autorizado por un Comité de Ética, que entre otros aspectos, verifica que se utilice el consentimiento informado válido, que se tomen medidas para minimizar los riesgos de los participantes y que exista un equilibrio entre riesgo-beneficio, dando mayor importancia al segundo (Berman, 2002).

Consentimiento informado

El consentimiento informado tiene el propósito de proporcionar a las personas la oportunidad de tomar decisiones libres e informadas sobre su participación en un estudio, promoviendo los principios de autonomía, libertad de elección y racionalidad (Froomkin, 2019; Serrano Diaz, Guio Mahecha y Paez Leal, 2016). Es un documento con perspectiva legal y política, donde el participante le da permiso al investigador de tratar sus datos con un fin específico (Breen, Ouazzane y Patel, 2020).

Su uso surge en el marco de la experimentación en la Segunda Guerra Mundial, en el que algunos grupos fueron explotados, surgiendo la necesidad de proteger la vida privada de las personas mediante instrumentos jurídicos como la Declaración Universal de los Derechos Humanos (Breen *et al*., 2020; Mendoza Enríquez, 2018).

Para que un consentimiento sea válido este debe ser informado, específico, explícito, inequívoco, auditable, otorgado de forma libre y retractable (Breen *et al*., 2020). De igual forma, se requiere que la persona que debe tomar la decisión sea capaz y competente para otorgarlo (Custers, Dechesne, Pieters, Schermer y van der Hof, *et al*., 2018).

Con la digitalización de datos históricos y la planeación de usos futuros, los consentimientos muchas veces abarcan el uso de datos pasados, presentes y futuros, complicando su función así como la protección de los derechos de los participantes (Schneble, Elger y Shaw, 2019).

Dependiendo de su cobertura en el tratamiento de datos se pueden distinguir distintos tipos de consentimiento informado: 1) El consentimiento específico reporta a los participante el uso único y puntual que se le darán a sus datos; 2) El consentimiento amplio pide la autorización para un uso específico y estudios secundarios de un área determinada; 3) El consentimiento abierto o general pide el uso sin restricción de los datos para proyectos futuros de cualquier tipo; y 4) El consentimiento dinámico en el que se mantiene la comunicación con el participante para involucrarlo y obtener su autorización para cada proyecto de investigación del que se requiera su información (Price y Cohen, 2019; Serrano Diaz *et al*., 2016).

Existe la crítica ética sobre algunos tipos de consentimiento informado, como el amplio y el general, cuestionando si respetan la autonomía y el derecho a oponerse al uso de datos, además de ponerse en duda la protección de la privacidad, ya que se da el acceso para cualquier uso de información pasada, presente y del futuro en cualquier momento y espacio dificultando controlar el alcance y tipo de resultados (Serrano Diaz *et al*., 2016).

Un caso especial referente al tipo de consentimiento que debe aplicarse es el de los biobancos. Los biobancos son cualquier colección de muestras biológicas que serán utilizados en investigación y que en muchas ocasiones se utilizan en diferentes proyectos por lo que se suele utilizar el consentimiento amplio o el general con los donadores de muestras (Cusí, 2014), lo que representa un riesgo de identificación importante y violaciones a los derechos que se suele justificar con el beneficio social que se obtiene a partir de la investigación en biomedicina (Serrano Diaz *et al*., 2016). Desde la perspectiva ética se propone el uso del consentimiento informado específico limitando la utilización de las muestras únicamente para el proyecto para las que fueron solicitadas o solicitar un consentimiento dinámico que permita autorizar o negar el uso de datos para cada proyecto planeado respetando la autonomía y anonimato de los donadores (Cusí, 2014; Serrano Diaz *et al*., 2016).

Medidas de seguridad para la información

Existen medidas de seguridad técnicas, físicas y administrativas para proteger la información de los usuarios de salud. Las medidas administrativas consisten en la gestión, soporte y revisión de la seguridad de la información, incluyendo su clasificación y la capacitación del personal en materia de protección de datos personales (Alfaro, 2012). Como medidas técnicas se encuentran la creación de usuarios y contraseñas, el acceso controlado y limitado de acuerdo con las funciones de cada responsable, contar con un software seguro y con recursos informáticos para la gestión de comunicación y manejo de datos (Alfaro, 2012; El Kettani *et al*., 2018). Actualmente las cuentas de usuario con contraseña son la forma más común de limitar el acceso a los archivos médicos, sin embargo, en ocasiones las cuentas se comparten entre el mismo personal de salud y por lo tanto deben integrarse nuevos mecanismos de seguridad (El Kettani *et al*., 2018). Algunas de las medidas de seguridad física consisten en evitar el acceso no autorizado, proteger los equipos dentro y fuera de la organización y dar mantenimiento a equipos e instalaciones (Alfaro, 2012).

Por otra parte, el tratamiento de datos personales requiere de métodos como la anonimización, desidentificación, seudonimización, transformación y el cifrado para proteger la privacidad (Krishna, Kelleher y Stahlberg, 2007). La anonimización consiste en eliminar los datos personales y que se pierda el vínculo con la persona a la que se refieren, aunque con esta medida se pierde la oportunidad de verificar la información e incluso la adición de datos recopilados posterior al registro (Berman, 2002). La desidentificación consiste en eliminar campos específicos que permiten la identificación de una persona, combinada con otras técnicas como el cifrado se puede volver a vincular la información con la persona correspondiente (Berman, 2002; El Kettani *et al*., 2018). La seudonimización consiste en remplazar los datos personales por otros atributos, de modo que la reidentificación no es posible a menos que se cuente con información adicional que debe mantenerse por separado y bajo clave (Meszaros y Ho, 2021; Rumbold y Pierscionek, 2017). Las técnicas de transformación de datos cambian los valores originales y correlaciones

de forma irreversible por lo que supone la pérdida de cierta información mientras se mantienen las relaciones de interés (Krishna *et al*., 2007). Los algoritmos de cifrado o encriptación cambian la información a un código, cuya capacidad de descifrado dependerá de la cantidad de datos y la calidad de la clave (El Kettani *et al*., 2018; Krishna *et al*., 2007).

En cualquiera de los métodos se debe considerar que la exclusión de datos conlleva el riesgo de afectar las inferencias o conclusiones resultantes de los análisis y que pese al método utilizado no se puede garantizar al 100 por ciento la privacidad, ya que al combinarse con otras fuentes de información y con técnicas de inteligencia artificial es viable la reidentificación (El Kettani *et al*., 2018; Krishna *et al*., 2007; Li *et al*., 2011).

Protección legal de la información

El derecho a la protección de datos personales, sustentado en el derecho a la privacidad, busca garantizar que cualquier persona ejerza su poder de decisión y control sobre la información que la involucra (Gómez Sánchez, 2020).

El derecho a la privacidad se establece a nivel mundial en el Artículo 12 de la Declaración Universal de los Derechos del Humanos, en el que se indica "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Declaración Universal de los Derechos Humanos, 1948; Gómez Sánchez, 2020).

En la actualidad, la mayoría de los países cuenta con leyes para la protección de datos que regulan en qué condiciones se puede acceder a la información de otras personas, cómo debe ser el tratamiento de los datos personales, cómo debe garantizarse la confidencialidad de la información y cómo se deben manejar las violaciones de la privacidad (Fonseca, 2017; Vayena y Blasimme, 2017).

Uno de los pioneros en la protección de datos personales es la Unión Europea, con el Reglamento General para la Protección de Da-

tos (GDPR, por sus siglas en inglés). En el GDPR se establece que el tratamiento de datos de salud está prohibido a menos que se cuente con el consentimiento explícito de la persona, que se requiera de la información para la atención médica o por razones de salud pública (Bondre *et al*., 2021).

En el caso de México, su marco legal es un modelo híbrido basado en las leyes europeas y de Estados Unidos (Arellano López, 2020). El derecho a la protección de datos personales se reconoce a nivel constitucional en el Artículo 6 y en dos leyes específicas para el tratamiento de datos personales por organizaciones públicas y privadas, la Ley General de Protección de Datos en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de Particulares respectivamente (Arellano López, 2020; Mendoza Enríquez, 2018).

En la legislación se establece que el titular de los datos es la persona que los proporciona y que tiene derecho a la protección de su información, al acceso, rectificación, cancelación u oposición de sus datos (conocidos como derechos ARCO) (Alfaro, 2012; Mendoza Enríquez, 2018). Mientras que el responsable de la información es la persona física o moral que decide sobre el tratamiento de los datos personales y, por lo tanto, debe cumplir con los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad (Alfaro, 2012; Gómez Sánchez, 2020).

Sustentado en el derecho a la protección de datos personales surge el derecho al olvido o el derecho a ser olvidado, que consiste en hacer que se borre toda la información sobre una persona después de un tiempo determinado si ésta afecta a la vida actual de la persona considerando que su reputación no debe reducirse a hechos pasados (De Terwangne, 2012). Si bien, se ha tratado de regular el derecho al olvido digital, sobretodo en países europeos en los que se reconoce el derecho a solicitar que los datos personales no figuren en los resultados de una búsqueda digital, el uso de Internet complica su aplicación debido a su gran capacidad de almacenamiento, que permite guardar los datos de forma permanente y que el costo de borrarlos sea mayor que el de almacenarlos (De Terwangne, 2012; Moreno Bobadilla, 2019). Además la eficacia y velocidad de los buscadores permiten obtener toda la información relacionada con una persona disponible en Internet con el simple hecho de

teclear su nombre (De Terwangne, 2012). Otra dificultad para su cumplimiento son los archivos públicos electrónicos de noticias, en el que el derecho al olvido se opone al derecho de libertad de expresión, al derecho de prensa y al derecho a la información pública; de lo anterior han surgido propuestas como desvincular el nombre de la persona a la búsqueda de la noticia, para que la relación entre el hecho y el protagonista no sea fácil de establecer sin tener la necesidad de eliminar la información (Maqueo Ramírez, 2019; Moreno Bobadilla, 2019). Tomando como base el principio de finalidad en el tratamiento de datos, una vez que se han cumplido los fines de su utilización, la información debe ser borrada o anonimizada, como si estos tuvieran una fecha de caducidad lo cual podría ser aplicado a lo digital, aunque representa grandes costos y un proceso complejo (De Terwangne, 2012). En México, el abordaje del derecho al olvido digital permanece inconcluso, sin legislación especial y sin un régimen de obligaciones para los intermediarios de Internet (Maqueo Ramírez, 2019).

Por otra parte, los expedientes clínicos están regulados por la Norma Oficial Mexicana NOM-004-SSA3-2012, junto con la Ley General de Salud y la Ley Federal de Protección de Datos Personales en Posesión de Particulares. En los que se establece que los expedientes son propiedad de la institución o del prestador de servicios que los genera, aunque el usuario sigue siendo el titular y tiene el derecho de la protección y confidencialidad de sus datos. Siempre que sean utilizados se deberá cuidar la no identificación del titular y se debe contar con el consentimiento informado, al menos que sea para un fin médico asistencial (Mier y Delgadillo, 2018).

En cuanto a la información registrada a partir de dispositivos electrónicos y aplicaciones, ésta debe ser regulada mediante los términos de servicios y avisos de privacidad que se exponen a los titulares de los datos (Schneble *et al*., 2019). Dichos avisos deben de presentarse en lenguaje claro y comprensible, en un formato que facilite su entendimiento (Alfaro, 2012). De forma contraria a la sugerida, los textos que se muestran hoy en día son largos, redactados en un contexto legal y con un lenguaje técnico que dificultan su comprensión por la población general (Schneble *et al*., 2019). Adicionalmente, sin un conocimiento previo, es difícil distinguir que sitio o aplicación ofrece una mejor protección de

privacidad que otro, por lo que generalmente se otorga la autorización sin la lectura profunda y el análisis adecuado (Custers *et al*., 2018).

Conclusiones

Existe un gran potencial en el tratamiento de datos de salud para beneficio de la población, con el inconveniente de no poder asegurar que las técnicas de anonimización así como las medidas de seguridad de la información puedan proteger de manera correcta la identidad de los usuarios de la salud (Froomkin, 2019).

Los riesgos que conlleva el acceso y uso sin medidas de seguridad de los datos de salud pueden ser la discriminación, marginación, explotación de grupos específicos, la pérdida de autonomía y dignidad humana (Malgieri y Niklas, 2020).

Los proveedores de salud, investigadores y personal relacionado deben reconocer la responsabilidad que tienen con los usuarios, principalmente respetando su confidencialidad. Siempre deben actuar de acuerdo con los principios éticos fundamentales de beneficencia, no maleficencia, autonomía y justicia (Rumbold y Pierscionek, 2017). Además de conocer las regulaciones que existen para la protección de datos como parte de el ejercicio profesional (Malgieri y Niklas, 2020).

El consentimiento informado es la herramienta más viable para respetar la autonomía de las personas, para que estos puedan mantener el control sobre sus datos. Por lo que su uso debería ser generalizado así como la revisión exhaustiva de los riesgos y beneficios del tratamiento de datos por parte de los especialistas, investigadores y Comités de Ética (Froomkin, 2019).

Finalmente, el valor de la información personal es incalculable, diferente para cada persona y situación, por lo que los custodios de datos no deben inferir que mientras alguien no se identifique no puede verse afectado o que estará de acuerdo con el uso de su información para cualquier propósito.

Bibliografía

Alfaro, J. G. P. (2012). El derecho a la protección de datos personales y la implementación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Epikeia. Derecho y política* (19). Disponible en: https://epikeia.leon.uia.mx/old/numeros/19/epikeia19-proteccion_de_datos_personales.pdf

Arellano López, C. A. (2020). El derecho de protección de datos personales. *Biolex. Revista jurídica del Departamento de Derecho*, 12 (23), 127–136. https://doi.org/10.36796/biolex.v0i23.194.

Berman, J. J. (2002). Confidentiality Issues for Medical Data Miners. *Artificial Intelligence in Medicine*, 26 (1-2), 25-36. https://doi.org/10.1016/S0933-3657(02)00050-7.

Boilson, A., A. Staines, R. Connolly, J. Connolly y P. Davis (2018). Transforming Health through Big Data: Challenges and Considerations. *UK Academy for Information Systems Conference Proceedings 2018*, 12.

Bondre, A., S. Pathare y J. A. Naslund (2021). Protecting Mental Health Data Privacy in India: The Case of Data Linkage With Aadhaar. *Global Health: Science and Practice*, 9 (3), 467-480. https://doi.org/10.9745/GHSP-D-20-00346.

Breen, S., K. Ouazzane y P. Patel (2020). GDPR: Is your consent valid? *Business Information Review*, 37 (1), 19-24. https://doi.org/10.1177/0266382120903254.

Cusí, V. (2014). Consentimiento informado dinámico versus consentimiento amplio en biobancos. *Bioètica & debat: tribuna abierta del Institut Borja de Bioètica*, 21 (74), 14-19.

Custers, B., F. Dechesne, W. Pieters, B. W. Schermer y S. van der Hof (2018). Consent and Privacy. En A. Müller y P. Schaber (eds.). *The Routledge Handbook of the Ethics of Consent* (pp. 247-258). Londres: Routledge.

Declaración Universal de los Derechos Humanos (1948). *Declaración Asamblea General de las Naciones Unidas*, 10.

De Terwangne, C. (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. *IDP. Revista de Internet, Derecho y Política*, 13, 53-66. Disponible en: https://www.redalyc.org/pdf/788/78824460006.pdf

Díaz de León Castañeda, C., y J. Góngora Ortega (2020). eSalud en servicios de salud públicos en México: Estudio de caso. *Región y sociedad*, 32, e1256. https://doi.org/10.22198/rys2020/32/1256.

El Kettani, A., S. Housban, Z. Serhier y M. B. Othmani (2018). Confidentiality in Electronic Health Records Systems: A Review. *Journal of Medical and Surgical Research*, 5, 551-554.

Flores-Hernández, S., L. R. Mendoza-Alvarado, W. I. Vieyra-Romero, E. Moreno-Zegbe, A. C. Bautista-Morales y H. Reyes-Morales (2019). La condición indígena en los servicios de salud: Comparación de la calidad en la atención 2012-2018 para la población en pobreza. *Salud Pública de México*, 61 (6), 716. https://doi.org/10.21149/10562.

Fonseca, C. F. A. (2017). Big Data: El valor de la información personal y la privacidad. *Ciencia, Innovación y Tecnología*, 3, 63–72.

Froomkin, A. M. (2019). Big Data: Destroyer of Informed Consent. *Yake Journal of Health Policy, Law, and Ethics*, forthcoming. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3405482.

Geri, L., y J. N. Lafferrière (2014). La confidencialidad médica ante las tecnologías de la información: Comentario al caso "Sorrell v. IMS Health Inc.". disponible en: https://repositorio.uca.edu.ar/handle/123456789/9098

Gómez Sánchez, M. A. (2020). La protección de datos personales en México. Cambios evolutivos a 10 años de su inclusión a nivel constitucional. *Revista Mexicana de Ciencias Penales*, 3 (10), 47-58.

Gutiérrez, J. P., I. Heredia-Pi, M. I. Hernández-Serrato, B. E. Pelcastre-Villafuerte, P. Torres-Pereda y H. Reyes-Morales (2019). Desigualdades en el acceso a servicios, base de las políticas para la reducción de la brecha en salud. *Salud Pública de México*, 61 (6), 726. https://doi.org/10.21149/10561.

Howe Iii, E. G., y F. Elenberg (2020). Ethical Challenges Posed by Big Data. *Innovations in Clinical Neuroscience*, 17 (10-12), 24-30.

Kaplan, B. (2014). How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2510013.

Kaplan, B. (2015). Selling Health Data: De-Identification, Privacy, and Speech. *Cambridge Quarterly of Healthcare Ethics*, 24 (3), 256-271. https://doi.org/10.1017/S0963180114000589.

Karasneh, R. A., S. I. Al-Azzam, K. H. Alzoubi, S. S. Hawamdeh y S. M. Muflih (2019). Patient Data Sharing and Confidentiality Practices of Researchers in Jordan. *Risk Management and Healthcare Policy*, 12, 255-263. https://doi.org/10.2147/RMHP.S227759.

Krishna, R., K. Kelleher y E. Stahlberg (2007). Patient Confidentiality in the Research Use of Clinical Medical Databases. *American Journal of Public Health*, 97 (4), 654-658. https://doi.org/10.2105/AJPH.2006.090902.

Li, F., X. Zou, P. Liu y J. Y. Chen (2011). New Threats to Health Data Privacy. *BMC Bioinformatics*, 12 (S12), S7. https://doi.org/10.1186/1471-2105-12-S12-S7.

Malgieri, G., y J. Niklas (2020). Vulnerable Data Subjects. *Computer Law & Security Review*, 37, 105415. https://doi.org/10.1016/j.clsr.2020.105415.

Maqueo Ramírez, M. S. (2019). El derecho al olvido digital desde la perspectiva de la Unión Europea y la viabilidad de su extrapolación al caso de México. *Latin American Law Review*, 3, 79-97. https://doi.org/10.29263/lar03.2019.04.

Martínez-García, D. N., V. M. Dalgo-Flores, J. L. Herrera-López, E. I. Analuisa-Jiménez y E. F. Velasco-Acurio (2019). Avances de la inteligencia artificial en salud. *Dominio de las Ciencias*, 5 (3), 603. https://doi.org/10.23857/dc.v5i3.955.

Medina-Gómez, O., y O. López-Arellano (2019). Informalidad laboral y derecho a la salud en México, un análisis crítico. *Ciência & Saúde Coletiva*, 24 (7), 2583-2592. https://doi.org/10.1590/1413-81232018247.14342017.

Mendoza Enríquez, O. A. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: Desafíos y cumplimiento. *Revista IUS*, 12 (41), 267-291.

Meszaros, J., y C. Ho (2021). AI Research and Data Protection: Can the Same Rules Apply for Commercial and Academic Research under the GDPR? C*omputer Law & Security Review*, 41, 105532. https://doi.org/10.1016/j.clsr.2021.105532.

Mier, C. H., y V. T. Delgadillo (2018). Regulación del acceso al expediente clínico con fines de investigación en México. *Revista CONAMED*, 22 (1), 27-31.

Mittelstadt, B. D., y L. Floridi (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Science and Engineering Ethics*, 22 (2), 303-341. https://doi.org/10.1007/s11948-015-9652-2.

Moreno Bobadilla, Á. (2019). El derecho al olvido digital: Una brecha entre Europa y Estados Unidos. *Revista de Comunicación*, 18 (1), 259-276. https://doi.org/10.26441/RC18.1-2019-A13.

Popescu, I. G., G. Sechel, F. G. Leaşu, M. M. Ţânţu, B.-V. Cotoi y L. M. Rogozea (2018). Correlations on the Protection of Personal Data and Intellectual Property Rights in Medical Research. *Rom J Morphol Embryol*, 59 (3), 1001-1005.

Price, W. N., e I. G. Cohen, I. G. (2019). Privacy in the Age of Medical Big Data. *Nature Medicine*, 25 (1), 37-43. https://doi.org/10.1038/s41591-018-0272-7.

Rumbold, J. M. M., y B. K. Pierscionek (2017). A Critique of the Regulation of Data Science in Healthcare Research in the European Union. *BMC Medical Ethics*, 18 (1), 27. https://doi.org/10.1186/s12910-017-0184-y.

Schneble, C. O., B. S. Elger y D. M. Shaw (2019). All Our Data Will Be Health Data One Day: The Need for Universal Data Protection and Comprehensive Consent (Preprint). *Journal of Medical Internet Research*. https://doi.org/10.2196/16879.

Serrano Diaz, N., E. Guio Mahecha y M. C. Paez Leal (2016). Consentimiento informado para biobancos: Un debate ético abierto. *Revista de la Universidad Industrial de Santander. Salud*, 48 (2), 246-256. https://doi.org/10.18273/revsal.v48n2-2016010.

Sugiarti, I., y D. Prodi III (2020). Legal Protection of Patient Rights to Completeness and Confidentiality in Management of Medical Record Documents. *Advances in Health Sciences Research*, 26, 179–191.

Vayena, E., y A. Blasimme (2017). Biomedical Big Data: New Models of Control Over Access, Use and Governance. *Journal of Bioethical Inquiry*, 14 (4), 501-513. https://doi.org/10.1007/s11673-017-9809-6.

Recibido: 14 de enero de 2022
Aceptado: 20 de marzo de 2022