

ANÁLISIS DE LA UTILIDAD DEL DERECHO DE
PORTABILIDAD DE DATOS PERSONALES PARA
LA GARANTÍA DEL DERECHO A LA SALUD,
A LA LUZ DEL REGLAMENTO GENERAL DE
PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA
Y LA LEY GENERAL DE PROTECCIÓN DE DATOS
PERSONALES EN POSESIÓN DE SUJETOS
OBLIGADOS DE MÉXICO

ANALYSIS OF THE USEFULNESS OF THE RIGHT OF
PORTABILITY OF PERSONAL DATA FOR THE GUARANTEE
OF THE RIGHT TO HEALTH, CONSIDERING THE GDPR AND
THE GENERAL LAW OF PROTECTION OF PERSONAL DATA IN
POSSESSION OF OBLIGED SUBJECTS OF MEXICO

ANA GUADALUPE OLVERA-ARELLANO

Doctoranda en el Programa de Doctorado en Derecho y Ciencias
Sociales de la Universidad Nacional de Educación a Distancia

Sumario: *I. Antecedentes. II. Marco normativo. III. Elementos del derecho a la portabilidad. IV. Análisis de los medios para ejercer el derecho a la portabilidad en el ámbito sanitario mexicano. V. Conclusiones. VI. Bibliografía*

Resumen: Con la publicación en el Diario Oficial de la Unión Europea del Reglamento General de Protección de Datos Personales (2016) y en el Diario Oficial de la Federación de la República Mexicana de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017), sobrevino la positivización del derecho a la portabilidad de datos personales, que ya encontraba antecedentes en el campo de las telecomunicaciones.

Sin embargo, los elementos subjetivos y objetivos de este derecho y que afectan a la totalidad del ciclo de vida del dato personal, nos dan cuenta de las muchas limitaciones existentes para su ejercicio y garantía, cuestión que además encuentra detalles específicos dependiendo de la materia que se trate.

En ese sentido, el presente pretende analizar si el ejercicio de este derecho, tal y como se encuentra previsto en las normas mencionadas que se encuentran vigentes, resulta beneficioso para los usuarios de los sistemas de salud o si, por el contrario, representa una carga.

Palabras clave: derecho de portabilidad; derecho a la salud; expediente clínico; derecho de protección de datos personales.

Abstract: With the publication in the Official Gazette of the European Union of the General Regulation of Protection of Personal Data (2016) and in the Official Gazette of the Federation of the Mexican Republic of the General Law of Protection of Personal Data in Possession of Obligated Subjects (2017), ensued the positivization of the right to the portability of personal data, which already found antecedents in the field of telecommunications.

However, the subjective and objective elements of this right affect the entire life cycle of personal data and give us an account of the many existing limitations that allow its exercise and guarantee, an issue that also finds specific details depending on the matter.

In this sense, the present intends to analyze if the exercise of this right, as it is foreseen in the mentioned norms that are in force, is beneficial for the users of the health systems, or if on the contrary, it represents a burden.

Keywords: portability right; right to health; medical records; right to protection of personal data.

Recepción original: 01/03/2022

Aceptación original: 23/04/2022

I. ANTECEDENTES

Con el desarrollo de la tecnología, cualquier información, aún y cuando se trate de una de naturaleza tan delicada como lo es la relativa al estado de salud, puede ser procesada, almacenada y transmitida a terceros que, en un principio, parecería que no tienen injerencia en

su tratamiento. Ello pone en grave riesgo a su titular, ante la inminente violación a su esfera íntima.

A este respecto, la portabilidad de datos, como cualquier otro derecho para cuya garantía, externalización o ejecución se requiere de la tecnología expresada por ejemplo en sistemas interoperables, viene a resignificar la característica de la universalidad de los derechos humanos. Se trata de un derecho de carácter instrumental que permite garantizar la universalidad de los derechos a cuyo ejercicio resulte beneficioso, como lo es el de la salud.

Así, encuentra su antecedente en la necesidad de los usuarios de servicios digitales de trasladar su lista de amigos, direcciones de correo electrónico y otro tipo de datos personales que brindan al hacer uso de ellos (Zanfiri, 2012:1). Otro antecedente importante es El Proyecto de Portabilidad de Datos, cuya creación en 2007 perseguía la finalidad de hacer posible este mecanismo. Sin embargo, aunque relevantes para su entendimiento, este artículo está centrado en el derecho positivizado en las normas de protección de datos personales.

Además, como antecedente directamente ligado a la importancia que reviste que el derecho a la portabilidad se garantice de forma adecuada, tenemos la ciencia ciudadana como la interpreta Quinn (2018:1) en el entendido de que reviste gran utilidad que los datos sean portables por su propio titular, teniendo la potestad de transferirlos a diversas instituciones de investigación, lo que ahora es posible lograr por los avances tecnológicos y de una forma diferente a la que el derecho de acceso nos faculta, para no solo transmitirlos, sino reunirlos, agruparlos y estudiarlos de formas distintas a las tradicionales, mediante la interacción de personas con intereses similares, debiendo cumplir con requisitos tales como la capacidad de registrar datos, de almacenarlos, de acceder a ellos y de que puedan transferirse.

II. MARCO NORMATIVO

Si bien es cierto que autores como Egan (2019:3) identifican la portabilidad como un principio que permite disponer de los propios datos personales para compartirlos con otro proveedor de servicios, incentivando la competencia de servicios en línea y que nuevos servicios emerjan, o bien, el Proyecto de Portabilidad de Datos (s.f) que conceptúa a la acción como una capacidad de las personas de reusar sus datos personales en aplicaciones interoperables o autores que como Ursic (2018:59) la consideran como una regla de la transferen-

cia de datos, no cabe duda de que se trata de un derecho fundamental reconocido ya en diversas disposiciones legales.

A) México

En México, únicamente se considera como un derecho que puede exigirse ante los sujetos obligados, es decir, cuya garantía depende de los entes públicos de gobierno y cuyos Lineamientos emitidos por el Sistema Nacional de Transparencia establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales (en lo sucesivo, Lineamientos de portabilidad y que fueron publicados en el Diario Oficial de la Federación en 2018). En contraposición, aún no se ha regulado lo respectivo en la Ley Federal de Protección de Datos Personales en Posesión de Particulares (2010). También es importante mencionar que no se encuentra previsto a nivel de la Constitución Política de los Estados Unidos Mexicanos (1917), como los derechos ARCO, sino únicamente en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSSO, 2017), por lo que su jerarquía se ve reducida.

De acuerdo con la LGPDPPSO, se trata de un derecho cuyo ejercicio persigue dos finalidades: la primera es que el titular de los datos obtenga del responsable del tratamiento una copia de los datos personales que le ha proporcionado en un formato electrónico estructurado y comúnmente utilizado, características que le permitirán seguir usándolos, sin que lo impida el responsable a quien se dieron los datos en primer lugar.

La segunda es que el titular pueda transmitir esos datos personales a otro responsable, siempre que se cumplan a su vez dos condiciones, a saber, la de que el tratamiento esté basado en el consentimiento del titular o en un contrato, y la segunda, que la información sea conservada en un sistema de tratamiento automatizado y que también sea comúnmente utilizado. En iguales términos lo consideran los Lineamientos de portabilidad, pero en el segundo supuesto especifica además que los datos debieron haber sido proporcionados por el titular de forma directa.

Los Lineamientos de portabilidad establecen como sujetos obligados a los mismos que la LGPDPPSO, por ser un derecho que se haya consagrado en ella, es decir, a cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, tribunales administrativos y fideicomisos y fondos públicos, todos ellos de los órdenes federal, estatal y

municipal cuando sea el caso, así como partidos políticos, siempre y cuando cuenten con sistemas en los que se lleve a cabo el tratamiento, que generen los formatos estructurados y comúnmente utilizados que requiere el ejercicio de este derecho.

De igual forma, la legislación mexicana en la materia se aplica sin perjuicio de las normas que tienen por objeto integrar los servicios digitales en trámites y servicios públicos y para compartir o reutilizar plataformas y sistemas de información en cuya posesión se encuentren los tres órdenes de gobierno y por supuesto es aplicable en la República Mexicana.

En cuanto a las causas de su procedencia, los Lineamientos de portabilidad establecen cinco condiciones de obligado cumplimiento, además de las características que deben revestir los datos objeto de tratamiento para que el titular pueda ejercer su derecho a la portabilidad, a saber:

1. Que el tratamiento se lleve a cabo a través de medios automatizados o electrónicos y en un formato estructurado y comúnmente utilizado.
2. Que los datos personales se encuentren en posesión del responsable o sus encargados.
3. Que los datos personales sean del titular que pretende ejercer el derecho o bien, de una persona fallecida siempre que el interés jurídico del promovente sea demostrado.
4. Que el titular haya proporcionado directamente sus datos personales al responsable y de forma activa y consciente, ya sea mediante un dispositivo tecnológico o bien, en el contexto del uso, la prestación de un servicio o la realización de un trámite.
5. Que su ejercicio no afecte los derechos y libertades de terceros.

B) España: normativa interna y de la Unión Europea

En la Unión Europea, podemos encontrar este derecho en los Reglamentos UE 2016/679 9 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1) y 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que

respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE, así como en España la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales¹, que además prevé la existencia de este derecho en servicios de redes sociales y servicios equivalentes.

A diferencia del caso mexicano, la legislación europea excluye de su ámbito de aplicación a los responsables que traten datos personales en el ejercicio de sus funciones públicas por lo que no puede ejercerse si la base de la legitimación del tratamiento de los datos es la necesidad de cumplir con una obligación legal aplicable al responsable o de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

Los Reglamentos UE 2016/679 y 2018/1725 establecen, en su exposición de motivos, que la finalidad de garantizar este derecho es dotar de mayores capacidades de control al titular acerca de sus propios datos personales si es que el tratamiento se lleva a cabo a través de medios automatizado, que les permita reutilizarlo o bien transmitirlo a un responsable distinto, con lo que coinciden autores como Zanfir (2012:1) al señalar que su garantía reduce las dificultades que los titulares de los datos tienen para autodeterminarse.

Los Reglamentos citados limitan su ejercicio si el tratamiento de los datos personales hace referencia al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable de tratamiento, cuestión en la que encontramos la primera gran diferencia con la legislación mexicana, pues como ya se ha dicho, en México está garantizado únicamente en la ley que protege datos personales en posesión de entes públicos y no así ante particulares responsables de tratamiento.

A su vez, tanto el Grupo de trabajo del Artículo 29 (en adelante, GT29 2017:3) como la Agencia Española de Protección de Datos (AEPD) (2017:22), reconocen como su propósito que el titular de los datos cuente con más control acerca de los datos personales que le conciernen y su manejo responsable. En lo que consideramos, se trata de fortalecer al derecho que tiene de autodeterminación informativa, al involucrarlo directamente en la tenencia y transmisibilidad de su

¹ Su artículo 17 determina que su ejercicio se llevará a cabo de acuerdo con lo que establece el Reglamento 2016/679 de la Unión Europea.

información a otro responsable, en los términos que mejor le convengan en entornos informáticos.

En cuanto a la temporalidad para el ejercicio del derecho a la portabilidad, la AEPD (2017:24), considera que, si bien ni el Reglamento UE 2016/679 ni el GT29 establecen criterio alguno, puede considerarse en principio que el responsable debería facilitar todos los datos en su haber de acuerdo con la obligación que marque la legislación en la materia específica, que es la que determina el plazo y no la obligación de garantizar el derecho a la portabilidad o “el adecuado mantenimiento de la relación contractual con el cliente”.

Resulta procedente también en los supuestos en que existiera una relación jurídica entre el responsable receptor y el titular, se dé cumplimiento a una disposición legal o a que el titular pretenda ejercer algún derecho. Además, según lo considera el GT29 (2017:9), el responsable deberá satisfacer la solicitud del titular a cabalidad, por lo que este puede inconformarse por este suceso.

A contrario sensu, se considerará que el ejercicio del derecho resulta improcedente si la información que se pretende portar es la inferida, creada o generada por el responsable del tratamiento a partir de los datos personales que ha recibido y que ha sido descrita en el apartado anterior.

Los Reglamentos UE 2016/679 y 2018/1725 establecen que, en sus dos modalidades, este será ejercido si el tratamiento de los datos se basa en el consentimiento en el caso de que el titular lo haya otorgado para el tratamiento de sus datos para uno o varios fines específicos, si el tratamiento a su vez es necesario para el cumplimiento de un contrato en el que el titular sea parte o para la aplicación de medias precontractuales o si el titular dio su consentimiento para el tratamiento de datos personales sensibles permitida por el derecho de la Unión.

El segundo supuesto es que el tratamiento se efectúe a través de medios automatizados. Así, no se establece un derecho general a la portabilidad, por lo que forzosamente deben cumplirse alguna de las dos circunstancias descritas como supuestos de procedencia, por lo que los responsables no cuentan con la obligación de ofrecer la portabilidad (GT29, 2017:10).

Kuebler-Wachendorff et al (2021, 265, 266) los identifican como sub derechos que derivan de la portabilidad. Para explicar el origen de los datos, consideran que pueden recibirse directamente de su titular; pero pueden ser observados al recopilarse por tecnología de

sensores. Los inferidos, por otra parte, comprenden los generados a partir de aquellos que se reciben y observan.

A su vez, los datos predichos hacen referencia al análisis indirecto de la realidad, resultando en pronósticos de la conducta del titular. Continúan con el segundo supuesto, acerca de la transmisión de la información mediante un formato estructurado, de uso común y de lectura mecánica, que consideran como los requisitos mínimos para facilitar la interoperabilidad de los datos, que debe plantearse para salvar los obstáculos tecnológicos en el ejercicio del derecho.

Igual que la legislación mexicana, la europea en cita prohíbe el menoscabo del derecho del titular a obtener la supresión de los datos personales y a su vez, no implica que los datos personales que ha proporcionado para la ejecución de un contrato se supriman.

A mayor abundamiento, el GT29 (2017:8) interpreta que el titular de los datos puede continuar usando los servicios del responsable después de ejercido su derecho a la portabilidad y que esta acción no propicia ni la supresión automática de la información, ni su periodo de retención y conservación original, es decir, que mientras el responsable transmisor continúe tratando los datos personales, el titular puede ejercer los derechos aparejados, incluyendo el derecho al olvido, para cuyo ejercicio no puede utilizarse como medio para impedirlo al de portabilidad.

Según De Hert et al (2018:202) esto propicia una competencia real entre proveedores de servicios y evita, a su vez, la monopolización del Internet pues los autores exploran como buena práctica el establecimiento de plataformas multinivel, superando incluso a los formatos interoperables, en el que el centro del modelo será siempre el titular de los datos personales y quienes lo operarían, serían los proveedores de servicios que a su vez son responsables del tratamiento de los datos.

En este sentido, es pertinente comentar que de acuerdo con el criterio del GT29 (2017:8), una vez que el responsable receptor tenga ya los datos personales se le consideran como facilitados por el titular de estos y pueden ser, a su vez, objeto de portabilidad siempre que cumplan con los requisitos de procedencia que ya hemos expuesto.

III. ELEMENTOS DEL DERECHO A LA PORTABILIDAD

Ni la legislación ni la doctrina ofrecen un concepto exacto de este derecho, más bien describen las características que debe revestir para su ejercicio, si bien es cierto que autores como Chassang et al

(2018:298) consideran que se trata de una parte del derecho fundamental de protección de datos personales, que amplía el de acceso al mundo digital, pues aunque cuentan con profundas diferencias, toda vez que no se trata de mejorar el acceso y accesibilidad a los datos personales al empoderar a su titular sino que se espera que al mismo tiempo sea una herramienta de impulso de la economía de datos.

Abonan a esta teoría De Hert et al (2018:194, 201) al referir que este derecho es el reflejo de un valioso desarrollo y difusión que, centradas en el usuario, mejorarían su privacidad, así como la posibilidad de disfrutar lo que denominan “riqueza inmaterial” constituida por sus datos personales en el entorno de la economía de datos, por lo que la portabilidad es un elemento imprescindible para empoderarle hacia la propiedad de sus datos personales en lo que denominan escenario de fusión, esto es, que el derecho a la portabilidad deberá verse como amalgama de la diversidad de servicios digitales, convirtiéndolos así en segmentos interoperables del internet de las cosas.

Es decir, que este derecho permitiría a los usuarios de servicios digitales llevar consigo los datos que han ido acumulando de un servicio a otro que se ajuste mejor a sus necesidades (Van der Auwermeulen, 2017:59), o lo que nosotros asumimos como portar la identidad digital que se ha ido construyendo para un producto o servicio en particular y que se ve como la continuación de la personalidad física del individuo, cuestión que a la larga deberá ser regulada y que según Zanfir (2012:3) y Ursic (2018:42) es la raíz del derecho a la portabilidad al propiciar éste el libre desarrollo de la personalidad en un entorno distinto al tradicional, y cuya expresión inicial ya hemos estudiado en el capítulo anterior al referirnos a los derechos digitales garantizados en España, por ejemplo.

De esta suerte, continúa Van der Auwermeulen (2017:68), que se haya positivizado tiene como objetivo adicional, desarrollar confianza en la actividad económica que se lleva a cabo en ambientes digitales para a su vez, incentivar su desarrollo económico, además de que se propiciará la interacción de los usuarios al frenar los monopolios, lo que adicionalmente atraerá nuevos usuarios.

Así, los prestadores de servicio no tendrán otra opción que desarrollar mejores estrategias que ofrezcan una experiencia al usuario basada en la confianza en el servicio que recibe y de cómo se tratan sus datos (Datum Future, 2019:12), brindándoles oportunidades tales como diversificar y mejorar la oferta de servicios y productos.

De forma similar opina Puccinelli (2017:16), pues considera a la portabilidad de la información y, en general, de los datos personales,

como un elemento indispensable de la nueva economía digital y también del gobierno abierto toda vez que por la evolución de la tecnología propician su intercambio en formatos interoperables y, cuya consagración normativa, aunque resulta una novedad necesaria, también deja de manifiesto que falta la implementación de diversas medidas como normas técnicas, modalidades y procedimientos que permitan la garantía debida del derecho.

En los Lineamientos de portabilidad, el Sistema Nacional de Transparencia sostiene que la portabilidad por sí misma impone la obligación exigible al responsable de procesar, filtrar, seleccionar, extraer y diferenciar los datos personales que son objeto de portabilidad, por lo que la información que sea inferida, derivada, creada, generada u obtenida a partir del análisis de los datos personales recabados incluyendo aquella resultante de los procesos de personalización, recomendación, categorización, creación de perfiles o procedimientos similares, así como los pseudónimos siempre que no identifiquen directamente o vuelvan identificable al titular, así como los datos disociados, no serán objeto del ejercicio de este derecho.

Otros datos excluidos de transmisión a causa del ejercicio de este derecho son los protegidos por la propiedad intelectual y los secretos comerciales, que si bien es cierto se encuentran protegidos, ante una solicitud deberán negarse, pero no los que efectivamente correspondan a quien pretende ejercer su derecho a la portabilidad (GT29, 2017:14).

Por ello, se considera que la portabilidad supone un alto “nivel de abstracción de cualquier formato interno o propietario. Como tal, la portabilidad de los datos supone un estrato adicional del tratamiento de los datos por parte del tratamiento, con el fin de extraer los datos de la plataforma y filtrar los datos personales que no estén incluidos en el ámbito de la portabilidad, tales como datos inferidos o datos relacionados con la seguridad de los sistemas.” (GT29:20)

En este supuesto, es decir, de los datos procedentes de la aplicación de técnicas de *know how* del responsable (AEPD, 2017:23)², se entiende que quedan excluidos los que así hayan sido obtenidos, sin que puedan excluirse del ejercicio del derecho los proporcionados directamente por el titular o aquellos que resulten derivados directamente del desarrollo del servicio, o sea, los que surjan como consecuencia de

² Sostiene la misma opinión Quinn (2018:9) aunque también cree que ese tipo de datos podrían ser de especial interés para cuestiones sanitarias o de investigación científica, ya que puede implicar el descubrimiento de correlaciones y relaciones que serían de inmenso interés.

esta causa, pero no así los que sean producidos intencionalmente por el responsable mediante las técnicas referidas. Sin embargo, la información inferida deberá ser otorgada mediante el ejercicio del derecho de acceso, aunque no del de portabilidad (Datum Future, 2019:4).

Lo anterior se entiende toda vez que, en su definición, el derecho únicamente ampara aquella información que fue proporcionada directamente por su titular, y a la que hacemos referencia en este apartado, en fruto del ejercicio profesional del responsable. En este sentido, los Lineamientos de portabilidad imponen la obligación al responsable de analizar de la forma más amplia los datos personales que han de ser entregados al titular, teniendo como únicas excepciones las descritas en este apartado, debiendo entregar, por lo tanto, la mayor cantidad de metadatos generados y obtenidos a partir del tratamiento de los datos personales proporcionados directamente por el titular.

A este respecto, en las conclusiones de su estudio, Kuebler-Wachendorff *et al* (2021:270), consideran que sería ampliamente beneficioso aumentar el alcance de los datos que pueden ser portados, incluyendo los inferidos, pues ayudaría a empoderar al titular de los datos y solicitar nuevos servicios o bien personalizarlos. En este mismo sentido, Chassang *et al* (2018:298) explican que lo conveniente será analizar los casos de forma individual, para diferenciar desde el principio cuáles son los datos susceptibles para portar. En nuestra opinión deberían implementarse estrategias de privacidad por diseño y defecto para facilitar la tarea.

Otro de los elementos es el derecho que tiene el titular de, si así lo desea, transmitir sus datos a otro responsable de tratamiento, a través del primer responsable o bien, a obtenerlos y luego que el propio titular realice tal acción. De acuerdo con el GT29 (2017:5), este resulta crucial pues, además de coadyuvar con su capacitación y participación lo que evitará la retención, el derecho que nos ocupa se formuló con el objetivo de innovar para llevar a cabo intercambios de datos de forma segura y eficiente que permitiera el enriquecimiento de los servicios y experiencias de los titulares que son sus consumidores.

No obstante, autores como Florez y Blind (2020:2) y Lam y Liu (2020:2) piensan que este derecho tendrá efectos ulteriores a los descritos, por ejemplo, el de obligar a las plataformas a implementar soluciones técnicas para el ejercicio del derecho que podría además de generar competencia, el riesgo de que el titular de los datos abandone la plataforma y de que se vuelva confiable para el usuario, tanto el servicio como su proveedor, tal cual afirma Van der Auwermeulen, (2017:60).

Sin embargo, esto no debería verse como un peligro sino como la oportunidad de innovar y solucionar los problemas inherentes con la finalidad de mejorar sus productos y servicios y a la vez incrementar su prestigio y presencia en el mercado, por lo que los servicios y proveedores más transparentes en el tratamiento de los datos deberían ser los elegidos por usuarios cada día más informados y que ejercen su autodeterminación informativa (Van der Auwermeulen, 2017:60).

Abonan lo anterior las afirmaciones de Datum Future (2019:2), que cree que los conceptos de control y propiedad de los datos personales no serán del todo comprendidos ni significantes para sus titulares hasta que estos puedan portarlos de manera segura y ágil, siendo el ánimo de la garantía de este derecho brindarle mayor control sobre su información personal, promoviendo de forma indirecta la interoperabilidad y evitando los monopolios de datos y mercados de datos.

Quinn (2018:6), a su vez, considera trascendental para el ejercicio del derecho dos elementos. El primero, que exista el derecho a recibir información en un formato legible por máquina y el segundo, que se otorgue el derecho al titular de los datos para solicitar su transferencia directa a un responsable distinto de con quien mantiene la relación originaria, siendo esta opción la que cree conveniente pues es el responsable quien podría encontrarse más preparado para llevar a cabo la transferencia.

La AEPD (2017:22) considera que la portabilidad de datos es un complemento del derecho de acceso y que este actuaría como límite máximo al que puede referirse el primero, toda vez que mientras el de acceso se refiere a la totalidad de los datos objeto de tratamiento sin importar la legitimación de esta acción, el de portabilidad únicamente encuentra cabida mediante el consentimiento o la relación contractual y ahí es donde se encuentra la limitación del espectro de datos que pueden ser objeto de portabilidad.

Chassang et al (2018:298), lo concibe como un derecho que puede desarrollar de forma vertical u horizontal, dependiendo de cómo lo ejerza el titular. Es decir que, si solicita que sus datos se transmitan de responsable a un segundo responsable, elegido por sí, nos encontramos ante la portabilidad horizontal. Si, por el contrario, solicita que la información le sea entregada, será portabilidad vertical.

Como resulta notorio, el criterio de los autores toma como fundamento a los responsables del tratamiento de los datos, pues en el primero de los casos los equipara en ese nivel de control que ejercen sobre la información, por lo que considera que se encuentran en una relación equitativa de poder con respecto al tratamiento de la infor-

mación. En cambio, la relación vertical en el esquema nos da cuenta de cuánto se empodera el titular de los datos al recibir, en el formato ya descrito, su información personal, para transmitirla o reutilizarla de acuerdo con sus necesidades.

Consecuencia de estos estudios, los teóricos identifican distintos tipos de portabilidad. Por ejemplo, Datum Future (2019:5) da cuenta de una portabilidad bilateral, en la que los datos se comunican directamente de un responsable a otro. La segunda, denominada multilateral, en la que los titulares de los datos pueden portarlos a varios intermediarios o servicios similares que fueron creados específicamente para facilitar, en nombre del usuario, su transferencia a otros responsables que ofrecen servicios similares, que pueden ser consolidados o combinados.

Por otra parte, De Hert et al (2018:197) consideran que el derecho a la portabilidad se compone a su vez, de tres derechos: el primero, el que tiene el titular de los datos de recibir sin obstáculos sus datos personales; el segundo, a transmitirlos a otro responsable del tratamiento; y, finalmente, el que tiene a que sus datos se transmitan directamente entre controladores, es decir, sin mediar su intervención, siempre que sea técnicamente realizable.

De esta suerte, y como consecuencia de que las empresas y plataformas se vuelven cada vez más poderosos por el crecimiento de lo que Kuebler-Wachendorff et al (2021:265) llaman silos de datos, es que se reconoce este derecho para fortalecer la soberanía de los titulares de los datos, además de habilitar la interoperabilidad entre los servicios que se ofrecen en línea y que ellos, en ejercicio de su autodeterminación informativa, participen en la economía de datos al decidir en qué condiciones proporciona su información personal, De ahí que se establezca este derecho como fundamental en el Reglamento UE 2016/679.

IV. ANÁLISIS DE LOS MEDIOS PARA EJERCER EL DERECHO A LA PORTABILIDAD EN EL ÁMBITO SANITARIO MEXICANO

El titular puede ejercer su derecho a la portabilidad, identificado por ambas legislaciones como la potestad para recuperar los datos personales que le incumban y que haya proporcionado a un responsable en un formato estructurado, de uso común y lectura mecánica y a transmitirlo a otro responsable sin que el primero de ellos lo impida (Comisión Europea, 2017:1).

En este tema, la AEPD (2017:22) considera que, en efecto, quien puede ejercitar el derecho es el titular del producto o servicio contratado, es decir, el titular de los datos que al contratar ha autorizado el tratamiento, pero no los terceros o los sujetos autorizados que se encuentren relacionados con el servicio, cuestión que cabe distinguir de que el titular ejerza su derecho a través de un representante legal, que no debe confundirse con la figura descrita.

Por lo anterior, Zanfir (2012:3) consideró que, si bien el objetivo principal del derecho a la portabilidad es el libre desarrollo de la personalidad, el medio para lograrlo es a través de procesos técnicos directamente relacionados con la protección de los datos personales que, al mismo tiempo, garantice que los responsables del tratamiento compitan equitativamente entre sí.

El Sistema Nacional de Transparencia mexicano identifica como principales diferencias: (i) el medio en que se encuentran soportados los datos, pues en el caso del derecho de acceso pueden estarlo en cualquiera, pero para el ejercicio de la portabilidad se requiere que lo sean en medios electrónicos o automatizados; (ii) la legitimación del tratamiento, en el primer caso se ejerce independientemente de esta circunstancia, pero la portabilidad se acota al consentimiento o a una relación contractual.

En cuanto a la forma, muy relacionada con la anterior, el titular obtiene acceso independientemente de esta circunstancia, pero solo pueden ser objeto de portabilidad los datos que haya proporcionado directamente así como los metadatos asociados, cuestión que creemos limita bastante el ejercicio del derecho, contrario a lo que la doctrina y autoridades de control europeas consideran al brindar el beneficio de la interpretación más amplia a esta cuestión y que será explicada a detalle en apartados posteriores.

Por último, la modalidad en que el derecho puede ser ejercido y la forma en que los datos serán reproducidos para entregarlos, en el ejercicio del derecho de acceso no encuentra limitación, pero en el de portabilidad necesariamente hablamos de un formato electrónico estructurado y comúnmente utilizado que implique la reutilización o aprovechamiento de los datos.

Este último punto se encuentra relacionado con lo que implica el ejercicio del derecho. En el caso del derecho de acceso, no necesariamente tendrá como finalidad transferir la información obtenida, los que autores como Chassang *et al* (2018:300) consideran que, aunque el ejercicio de ese derecho no implica este tipo de acciones, no se encuentran limitadas más que por las limitaciones que la legislación

establezca, mientras que el de portabilidad tiene como característica intrínseca su retransmisión y reaprovechamiento de forma vertical y horizontal y para las finalidades que ya han sido explicadas, encontrando ambos además de otras causas, límites en su ejercicio en el respeto a los derechos y libertades de terceros.

Quinn (2018:16) reconoce importantes diferencias y limitaciones a este derecho. En el primer caso, se diferencia del de acceso porque en contraste con este además de proporcionar información inteligible esta deberá ser suministrada en un formato interoperable, más no compatible por las dificultades que ello implica, así como de los datos que pueden ser objeto del derecho y las bases jurídicas que legitiman su ejercicio, o su ámbito de validez territorial.

Van der Auwermeulen (2017:60), por su parte, realiza importantes acotaciones acerca de las desventajas que supone su positivización y garantía, entre las que menciona que sería perjudicial para la privacidad dado el poco control que pueden ejercer los usuarios sobre sus datos como consecuencia de la opacidad reinante en el proceso de portabilidad y su desconocimiento acerca del ejercicio de su derecho a la autodeterminación informativa y la protección de datos personales, exponiéndolo a peligros tales como el fraude de identidad. Además, considera al riesgo de violentar la propiedad intelectual toda vez que, como otros autores que ya hemos citado, considera que no se ha identificado en la legislación, de forma precisa, qué información está sujeta a la portabilidad de la que no, teniendo un mayor problema aquellas compañías cuyos servicios se basan enteramente, o en su mayoría, en el tratamiento de datos personales.

Datum Future (2019:5) identifica a su vez algunas barreras para su ejercicio, tales como que no existe una obligación clara de recibir datos mediante estos mecanismos, lo que podría generarles importantes gastos para implementar la tecnología que les permita leer la información portada; también que los usuarios se resistan al ejercicio de su derecho sobre todo por ignorancia, idea en la que coincide con Van der Auwermeulen (2017) y Zanfir (2012:2) que destacan lo importante que es la confianza en el proveedor de servicios y en los que ofrece, así como la transparencia con la que trata los datos personales.

Para consolidar este derecho, que de entrada autores como Ursic (2018:42) consideran endeble desde su origen legal, se propone que se ejerza de cuatro formas: estableciendo control sobre las transferencias de datos personales; permitiendo el uso y reutilización de los datos personales; permitiendo un mejor entendimiento de los flujos de datos; y, finalmente, que se facilite la equidad y se fomente el libre

desarrollo de la personalidad, incrementando el ejercicio del derecho a la transparencia en el tratamiento de los datos, como elemento complementario.

A mayor abundamiento, Lynskey (2020:506) identifica el fortalecimiento de los protocolos de seguridad de los datos personales como el mayor de los desafíos para garantizar el ejercicio de este derecho; habilitando, por ejemplo, controladores programados para identificar dudas razonables de la identidad de quien quiera ejercer el derecho, con el objetivo de confirmarla. Además, considera importante la realización de una evaluación de impacto en la que deberían preverse estas áreas de oportunidad.

Quinn (2018:10) hace un análisis interesantísimo respecto a las limitaciones del ejercicio de este derecho por la propia naturaleza con que fue concebido, por lo que, para conseguir información de interés para ser partícipe de un proyecto de investigación distinto, por ejemplo, podría ser imposible bajo el supuesto de la portabilidad, por más que quisiéramos acogernos a los beneficios del manejo de la información que implica esta figura.

Lo mismo sucedería con los datos de un paciente tratados para fines de medicina preventiva o del trabajo, pues recordemos que de acuerdo con el Reglamento UE 2016/679, difiere del simple consentimiento de su titular, que se considera así para no pedir el consentimiento de los titulares de continuo y que les beneficia al ver garantizado su derecho a la protección de la salud.

Deberán tener en cuenta siempre la clasificación de los datos de que se traten y efectuando las mejores prácticas para garantizar la seguridad pero también para la agilización del ejercicio del derecho, lo que para los responsables del tratamiento incluye la implementación de incentivos, la regulación específica en la materia e incluso, la educación a la población para el mejor aprovechamiento y garantía de este derecho, por lo que, en consecuencia, incentivaría la autodeterminación informativa del titular de los datos, facilitando su transferencia y promoviendo la innovación basada en los datos.

Sánchez-Caro y Abellán (2016:11) señalan que cuando el médico acepta atender a un paciente, adquiere el compromiso de asegurar la continuidad de sus servicios con la excepción de que este pierda la confianza en su labor. Si la situación se presentara, deberá comentarlo con el paciente o sus familiares y hacer lo posible por favorecer que un colega continúe con la atención, al que le transmitirá la información necesaria para tal efecto, con el consentimiento de quien deba otorgarlo, según sea el caso particular.

Para lograrlo, existen soluciones tecnológicas que hacen posible la interoperabilidad, entendida como la transmisión de datos entre sistemas de información heterogéneos, de la que uno de sus aspectos es la interoperabilidad semántica.

Uno de los pasos imprescindibles para alcanzarla es definir, por acuerdo, el conjunto de datos que, por su relevancia, deben estar contenidos en los diferentes informes clínicos que describen los procesos de atención sanitaria realizados a ciudadanos concretos en cualquier centro o servicio del Sistema Nacional de Salud. Esta homogeneidad es uno de los elementos de normalización que facilitan el intercambio entre sistemas diferentes al servicio de los ciudadanos.

Además de la contribución que supone la normalización de los contenidos de cara a hacer posible la interoperabilidad entre sistemas de información distintos, la instauración de modelos básicos, contrastados por expertos, como instrumento para recoger y presentar la información clínica de manera estandarizada, permite garantizar una homogeneidad en los contenidos de los documentos clínicos en el sistema sanitario público que facilita su comprensión y la más rápida localización de la información, tanto a los pacientes como a los profesionales sanitarios, con independencia del territorio donde deban ser atendidos o donde se haya generado la información, dando de esta forma cumplimiento al mandato de la Ley General de Salud (publicada en el Diario Oficial de la Federación el 07 de febrero de 1984), de que el Sistema Nacional de Salud cuente con cohesión y calidad.

Existen soluciones tecnológicas que hacen posible la interoperabilidad, entendida como la transmisión de datos entre sistemas de información heterogéneos, de la que uno de sus aspectos es la interoperabilidad semántica.

También deberá garantizar si fuera posible la interoperabilidad del formato en que se entreguen los datos personales para que estos puedan ser utilizados o comunicados de forma uniforme y eficiente, procurando que sus sistemas y servicios mantengan la capacidad de interoperar con otros, como cualidad que deberá preverse desde su diseño y para su ciclo de vida, de manera que el intercambio de información exista independientemente del lenguaje de programación o plataforma en la que se desarrolle.

La interoperabilidad, menciona Engels (2016:4), no debe confundirse con la portabilidad, pues la primera va más allá de la segunda, al ser su objetivo la interconexión de los usuarios independientemente de la plataforma que utilicen, pero la segunda, implica tomar los

propios datos y enviarlos a una plataforma distinta para no comenzar con el perfil de usuario desde una etapa inicial.

Así, Indarte (2012:317), considera a la interoperabilidad como una de las características esenciales de los sistemas de información en salud, ya que permite “la comunicación transversal y longitudinal a lo largo de la estructura de los servicios de salud, garantizando la confidencialidad y la integridad de la información intercambiada y su acceso oportuno” lo que a su vez asume como un desafío que de ser superado, permitiría “una gestión efectiva, eficiente y eficaz centrada en los ciudadanos”. Tal es su importancia que, continúa la autora, este concepto no debe analizarse solo desde el punto de vista informático, sino también del de salud en el que se ven involucrados principalmente tanto los profesionales de la salud como las autoridades que la regulan ya que, si se hace de forma correcta, se evitaría perder información valiosa acerca del estado de salud de los usuarios y a su vez, hacer menor cualquier riesgo potencial para ellos al impedir que el profesional de la salud tome decisiones basadas en información incompleta o parcial (2012, 318).

Por lo que hace a las condiciones técnicas, ya Lueders (2004:9) recomendaba como criterio indispensable que el software a adquirir o desarrollar debía ser uno mediante el que se garantizara la compatibilidad con estándares abiertos, concepto que hace referencia, según el mismo autor, al “conjunto de reglas y especificaciones que describen colectivamente el diseño o las características de funcionamiento de un programa o dispositivo, siendo publicado y puesto a disposición de la comunidad técnica de forma gratuita”, en contraste al código fuente abierto que se entiende como “un programa en el cual el código fuente está disponible para el uso del público en general y/o para la modificación de su forma de diseño original”, por lo que, al no ser un estándar abierto si bien puede interoperar, no quiere decir que tenga implementados los mismos estándares que otros programas de código abierto.

Engels (2016:4) asevera que el responsable debe observar, previo a la transmisión de los datos, que tanto el recién mencionado como el receptor han adoptado las herramientas indispensables para enlazarse y comunicarse eficientemente, así como las medidas de seguridad necesarias, los mecanismos de autenticación de exclusivo uso para este fin, los relativos al control para evidenciar el envío, recepción e integridad de los datos personales así como que las plataformas electrónicas o sistemas utilizadas para portar datos, que además de que envíen y reciban datos en formatos estructurados y comúnmen-

te utilizados, emitan un registro de cualquier operación realizada al respecto, incluyendo los relativos a los momentos en que se llevan a cabo, así como a los sujetos que en ellos intervienen.

Particularmente, el GT29 (2017:15), indica que deberá garantizarse que distinguen el derecho de portabilidad de otros, cumpliendo con el principio de información, como deben hacerlo también con otros principios de protección de datos y con otros derechos relacionados. Considera también como una buena práctica incluir información acerca del ejercicio de este derecho previamente a cesar la relación jurídica con el titular, ofreciéndole así la posibilidad de evaluar los datos existentes para determinar su destino. Igualmente recomienda a los responsables receptores brindar la relativa a qué datos son susceptibles de ser portados, lo que también coadyuva a afianzar la autodeterminación informativa en los titulares de los datos al limitar los riesgos para terceros y colaborar en su exactitud y calidad.

Zanfir (2012:4) propone analizar la importancia de la computación en la nube como medio para garantizar la portabilidad de datos pues contrario a lo que se supone, no aminorará la privacidad ni la protección de los datos, sino que se incentivaría la implementación de mejores y adicionales medidas de seguridad y en consecuencia se fortalecería la autodeterminación informativa al facilitar y robustecer el acceso y control que sobre sus datos tienen sus titulares, además de ser necesario el trabajo legislativo correspondiente con lo cual, según la autora, incluso volverá visible la importancia que tiene el derecho de protección de datos personales.

Por su parte, Ursic (2018:50) considera que se utilizan estos términos sin definir con el propósito de que la legislación permanezca tecnológicamente neutral, independiente de la tecnología que se utilice para dar cumplimiento a este mandato legal. Sin embargo, añade, puede convertirse en un obstáculo para la correcta transferencia de la información al no establecerse las condiciones y requisitos mínimos necesarios para llevar la tarea a cabo.

Es más, la interoperabilidad será el elemento clave para la implementación de la portabilidad, pues a su vez propiciará la ejecución de nuevos servicios desarrollados en beneficio de los consumidores y, en consecuencia, nuevas oportunidades de mercado y ventajas competitivas podrán ser alcanzada por los prestadores de servicios digitales (Datum Future, 2019:6; De Hert et al, 2018:194; Wang & Shah, 2017:20).

En ese sentido se pronuncia el GT29 (2017:18), pues contempla que los casos han de evaluarse individualmente para saber si se cuenta

con los medios que hagan viable la portabilidad de datos, es decir, que en un principio será un formato interoperable, si bien es cierto que el receptor no se encuentra obligado a aceptarlo ya que pueden existir diferencias técnicas, en cuyo caso se expondrá al titular esta dificultad, lo que se considerará como una negativa a atender la solicitud.

Así, antes de externarla, los responsables deben valorar opciones para garantizar el derecho, tales como la transmisión directa del conjunto de datos, hacerlo en partes o bien, mediante una herramienta automatizada que permita elegir los datos que resulten pertinentes. (GT29, 2017:18).

A su vez, los responsables pueden ofrecer mecanismos tales como la descarga directa de los datos o bien, la transmisión a otro responsable mediante una interfaz de programación de aplicaciones, el uso de un almacén de datos personales, contar con un tercero de confianza para su custodia, almacenamiento o concesión de permiso para su aprovechamiento por otro responsable y para procurar su transferencia, según sugiere la Comisión Europea (2017:1).

No obstante, los requisitos que la norma europea impone, lo cierto es que no establece condiciones específicas acerca del formato en que los datos deben transmitirse, por lo que diferirá dependiendo del sector que se trate, pero deberá procurarse que mediante ellos se procure la garantía del derecho a la portabilidad, por lo que deberán ser de lectura fácil pero no necesariamente compatibles, pero si interoperables pues esta es la obligación contenida.

Autores como Quinn (2018:7) consideran que algunos límites al concepto de “legibilidad de la máquina” deben ser considerados en la garantía de este derecho, siendo más bien cautos en su interpretación, pues según expone, no se impone la obligación al responsable de garantizar que los datos sean compatibles con todos los fines imaginables, lo que cree, podría ser un “elemento disuasorio para el procesamiento de datos en general” y que debe contemplarse más bien, como una responsabilidad compartida.

De no existir, el GT29 recomienda intercambiarlos en “formatos abiertos de uso común junto con metadatos útiles con el mejor nivel posible de granularidad, al tiempo que mantienen un alto grado de abstracción” (2017:20), sin que ello suponga la revelación de secretos industriales o información protegida por la norma de propiedad intelectual, por ejemplo, y tampoco resultaría adecuado utilizar formatos como el PDF.

También deberá ser cuidadoso en valorar en qué grado el formato utilizado dificultará la reutilización de esos datos al titular, explican-

do en todo caso las causas y conveniencia de lo decidido. Sin embargo, precisa que el procesamiento de metadatos adicionales no supone una justificación legítima solo para garantizar la portabilidad de los datos a futuro, alentando aun así la cooperación entre los miembros de diversos sectores para establecer normas y formatos interoperables ajustados a sus necesidades y a los requisitos de garantía de este derecho.

De esta suerte, y siendo la portabilidad en opinión del GT29 (2017:20) un tratamiento adicional y complementario al declarado inicialmente toda vez que no se lleva a cabo para lograr fines distintos a los señalados, esto debería incitar a los responsables a mantener de forma permanente los datos exactos y actualizados, para facilitar esta tarea.

Indarte (2012:327) propone que, para lograrla, deberían atenderse a los presupuestos mínimos tales como la normalización del registro de usuarios, la identificación de las instituciones prestadoras de servicios de salud, así como el conjunto de actos médicos, fármacos y servicios que se brindan a los usuarios y que se realizan en el sistema, usando codificaciones internacionales para facilitar la tarea, además del establecimiento de los estándares necesarios para que los sistemas se comuniquen.

En el tema que nos atañe, este trabajo debería ser realizado por profesionales sanitarios en conjunto con aquellos que lo sean en la gestión de datos e información, entendiéndose que, si se las características se logran, se beneficia directamente el titular de los datos en tanto le ofrecen un servicio de calidad y al mismo tiempo, le garantizan su derecho de protección de datos personales en sus diversas vertientes (Marco y Salvador, 2017: 2, 29 y 37).

V. CONCLUSIONES

El objetivo de reconocer la portabilidad, como otro derecho del espectro de la protección de datos, no es otro que el de reforzar la autodeterminación del titular de los datos, respecto de que quiere hacer con éstos.

El derecho a la portabilidad de datos puede representar una verdadera innovación para la garantía de otro derecho, así como del empoderamiento del titular de los datos, siempre y cuando se le dote de contenido, sobre todo tratándose del técnico indispensable para que se cumpla el objeto de su positivización.

La portabilidad es un derecho distinto al de acceso de los datos personales y para que el titular pueda ejercer su derecho con la mínima participación del responsable, este debería cumplir con los principios del tratamiento para que los datos se encuentren exactos, pertinentes y actualizados en todo momento, lo que a su vez quitará cargas innecesarias al responsable que retrasen la transmisión de los datos.

Otra diferencia importante entre los derechos de portabilidad y acceso, que ayuda a definir al primero, es que este únicamente nos permite conocer los datos que se proporcionaron al inicio de la relación jurídica y su objetivo además será el de proporcionarlos a otro responsable directamente o a través del titular de los datos como intermediario, para brindar un servicio similar.

Aunque los datos inferidos también son identificados como datos personales, toda vez que son productos del análisis llevado a cabo por los responsables por el que se descubrirán otros que incluso pueden llegar a ser sensibles pues darán cuenta de características de las personas tales como conductas, costumbres o el estado de salud, por concepto y determinación legal, éstos no pueden ser compartidos fundamentalmente por cuestiones económicas y de competencia, lo que evidencia que en el campo sanitario, el ejercicio del derecho de portabilidad de datos puede representar una carga para el titular de los datos en vez de una herramienta que le permita acceder a los servicios de salud de forma pronta y eficiente.

Dada la complejidad del Sistema Nacional de Salud mexicano, se aprecia la ventaja de contar con un esquema de interoperabilidad que facilite el flujo de información entre sus diversos actores.

La interoperabilidad, como característica también resulta fundamental si en México finalmente se implementara un expediente clínico electrónico único, siguiendo el ejemplo español y de otros países de la Unión Europea o de Latinoamérica incluso, ya que permitiría el acceso a ese archivo único a nombre del titular de los datos, en el que podrían reflejarse las diversas opiniones que emitan los profesionales de la salud en el área de su especialidad acerca de su estado de salud.

El responsable del tratamiento, sin importar si es un ente público o privado, debería procurar la modernización de sus sistemas para que paulatinamente los datos se traten en formatos interoperables comunes y estructurados de forma que, además de concebirlos privados por diseño y por defecto, también sean portables desde su origen, lo que sin duda beneficiaría a los usuarios de los servicios de salud pues, entre otras ventajas, verían agilizada su atención por no tener que estar sometidos a los tiempos de respuesta que marca la legislación.

Al mismo tiempo, la medida descrita coadyuvaría como un mecanismo de auditoría o rendición de cuentas al trabajo de los profesionales de la salud y que, sin tener motivo de incentivar la medicina defensiva, sí lo sería de procurar elaborar con pulcritud y apego a la legislación vigente un instrumento tan importante como lo es el expediente clínico.

A su vez, esta acción estimularía el ejercicio y garantía de otros derechos asociados como es el de acceso a la protección de la salud, al proveer de los medios para tener una atención oportuna y de calidad, así como a las opiniones de tantos facultativos como se considere conveniente, así como de otros que tienen estrecha relación tal como el de protección de datos personales al ser capaces de recibir información exacta y oportuna, de que los registros se conserven con la confidencialidad necesaria que a su vez se enlaza con el deber de secreto profesional, cuya violación puede derivar en responsabilidades de orden administrativo, civil o penal.

Igualmente, deben establecerse medidas de seguridad suficientes que permitan el acceso seguro tanto del médico como del paciente, lo que sin duda sí coadyuvaría a cumplir el objetivo planteado para la positivización del derecho a la portabilidad, es decir, empoderar al titular de los datos al tener verdadero control acerca del conocimiento de su estado de salud y de quién puede acceder a esa información, estableciendo para ello los controles suficientes que permitan saber quiénes y bajo qué circunstancias han tenido acceso a esos datos.

Finalmente, consideramos que debe trabajarse en estándares específicos para el sector salud, para que la portabilidad pueda ser integrada por diseño ya que los lineamientos fueron redactados de forma tan abierta que no responden a las necesidades particulares de los sectores a los que pertenecen los responsables del tratamiento de los datos personales.

VI. FUENTES DE CONSULTA

Bibliografía

- BOBBIO, N. (1991). *El tiempo de los derechos*. Madrid: Sistema.
- CENTRE FOR INFORMATION POLICY LEADERSHIP. (2017). *Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" adopted on 13 December 2016*. Obtenido de <https://www.>

informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf

- CHASSANG, G., SOUTHERINGTON, T., TZORTZATOU, O., BOECKHOUT, M., & SLOCKENBERGA, S. (2018). Data portability in health research and biobanking: legal benchmarks for appropriate implementation. *European Data Protection Law Review*, 4, 296-307.
- DATA PORTABILITY PROJECT P. (s.f.). Recuperado el 2021, de Data Portability Project: <http://dataportability.org/>
- DATUM FUTURE. (julio de 2019). *Data portability: what is at stake?* Obtenido de Datum Future: <https://www.datumfuture.org/wp-content/uploads/2019/07/Datum-Future-Data-Portability-July-2019.pdf>
- DE HERT, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sánchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, 193-203. doi:<https://doi.org/10.1016/j.clsr.2017.10.003>
- EGAN, E. (2019). *Data portability and privacy*. Facebook.
- ENGELS, B. (11 de junio de 2016). Data portability among online platforms. *Internet Policy Review*, 5(2). doi:10.14763/2016.2.408
- EUROPEAN BANKING FEDERATION. (2017). *European Banking Federation's comments to the Working Party 29 guidelines on the right to data portability*. Bruselas. Obtenido de https://www.ebf.eu/wp-content/uploads/2017/04/EBF_025448E-EBF-Comments-to-the-WP-29-Guidelines_Right-of-data-portabi.._.pdf
- FLÓREZ RAMOS, E., & BLIND, K. (2020). Data portability effects on data-driven innovation of online platforms: Analyzing Spotify. *Telecommunications Policy*, 44(9). doi:<https://doi.org/10.1016/j.telpol.2020.102026>.
- GANS, J. (junio de 2018). *Enhancing Competition with Data and Identity Portability. Policy proposal*. Brookings.
- INDARTE, S. (2012). Interoperabilidad. En J. Carnicero, & A. Fernández, *Manual de salud electrónica para directivos de servicios y sistemas de salud* (págs. 317-330). Santiago de Chile: Naciones Unidas, CEPAL, Sociedad Española de Informática de la Salud, Alianza para la sociedad de la información en América LATina y el Caribe.
- INDARTE, S., & PAZOS GUTIÉRREZ, P. (2011). *Estándares e interoperabilidad en salud electrónica: requisitos para una gestión sanitaria*

- efectiva y eficiente*. Santiago de Chile: Comisión Económica para América Latina y el Caribe.
- HOYOS CASTAÑEDA, I. M. (2017). Los derechos humanos en una época de crisis. En J. Saldaña Serrano, *Problemas actuales sobre derechos humanos. Una propuesta filosófica*. (págs. 133-154). México: Universidad Nacional Autónoma de México.
- KRÄMER, J., & STÜDLIN, N. (2019). Data portability, data disclosure and data-induced switching costs: Some unintended consequences of the General Data Protection Regulation. *Economics Letters*, 181, 99-103. doi:<https://doi.org/10.1016/j.econlet.2019.05.015>
- KUEBLER-WACHENDORFF, S., LUZSA, R., KRANZ, J., MAGER, S., SYRMOUDIS, E., MAYR, S., & GROSSKLAGS, J. (2021). The Right to Data Portability: conception, status quo, and future directions. *Informatik Spektrum*, 44, 264-272. doi:<https://doi.org/10.1007/s00287-021-01372-w>
- LYNSKEY, O. (2020). Article 20 Right to data portability. En C. Kuner, L. Bygrave, & C. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*. (págs. 497-507). Oxford University Press.
- MACGILLIVRAY, A., & SHAMBAUGH, J. (30 de septiembre de 2016). *Exploring data portability*. Obtenido de The White Huse (President Barack Obama): <https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability>
- MARCO CUENCA, G., & SALVADOR OLIVÁN, J. (2017). Representación del conocimiento en historia clínica electrónica: el caso de la Historia Clínica Digital del Sistema Nacional de Salud de España. *Scire*, 25-38.
- PÉREZ LUÑO, A. (2012). Bioética e intimidad, la tutela de los datos personales biomédicos. En A. Marcos del Cano, *Bioética y derechos humanos* (págs. 77-104). UNED.
- PUCCINELLI, O. (22 de enero de 2017). El derecho a la portabilidad de los datos personales. Orígenes, sentido y alcances. *Pensamiento constitucional*, 22. Obtenido de <https://2019.vlex.com/#vid/derecho-portabilidad-datos-personales-736214789>
- QUINN, P. (2018). Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science? *Global Jurist*, 18(2), 20180021. doi:<https://doi.org/10.1515/gj-2018-0021>

- SWIRE, P., & LAGOS, Y. (31 de mayo de 2013). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review. Ohio State Public Law Working Paper*. doi:<http://dx.doi.org/10.2139/ssrn.2159157>
- TURNER, S., GALINDO QUINTERO, J., TURNER, S., LIS, J., & TANCZER, L. (2020). The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *New Media & Society*, 1-21.
- URSIC, H. (2018). Unfolding the Newborn Right to Data Portability: Four Gateways to Data Subject Control. *Scripted*, 42-69. doi:[10.2966/scrip.150118.42](https://doi.org/10.2966/scrip.150118.42)
- VAN DER AUWERMEULEN, B. (2017). How to attribute the right to data portability in Europe: A comparative analysis of legislations. *ScienceDirect*, 33, 57-72. doi:<http://dx.doi.org/10.1016/j.clsr.2016.11.012>
- WANG, Y., & SHAH, A. (2017). *Supporting Data Portability in the Cloud Under the GDPR*. Carnegie Mellon University.
- WYNNE LAM, W., & LIU, X. (2020). Does data portability facilitate entry? *International Journal of Industrial Organization*, 69, 102564. doi:<https://doi.org/10.1016/j.ijindorg.2019.102564>
- ZANFIR, G. (2012). The right to Data portability in the context of the EU data protection reform. *International Data Privacy Law*, 1-14. doi:[10.1093/idpl/ips009](https://doi.org/10.1093/idpl/ips009)

Legislación y su interpretación

- CONSEJO, P. E. (16 de febrero de 2011). REGLAMENTO (UE) No 182/2011 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 16 de febrero de 2011 por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competen. *Diario Oficial de la Unión Europea*. Recuperado el 04 de octubre de 2021, de <https://www.boe.es/doue/2011/055/L00013-00020.pdf>
- CONSEJO, P. E. (23 de octubre de 2018). REGLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.o 45/2001 y la Decisión n.o 1247/2002/CE *Diario Oficial de la Unión*

Europea. Recuperado el 04 de octubre de 2021, de <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1725&from=fr>

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. (09 de agosto de 2019). *Diario Oficial de la Federación*. México. Obtenido de <https://tinyurl.com/y5tf5qc9>

GRUPO DE TRABAJO DEL ARTÍCULO 29. (2014). *Dictamen 05/2014 sobre técnicas de anonimización*. Bruselas: Grupo de trabajo sobre protección de datos del artículo 29.

GRUPO DE TRABAJO DEL ARTÍCULO 29. (2017). *Directrices sobre el derecho a la portabilidad de datos*. Grupo de trabajo sobre protección de datos del artículo 29.

INAI. (19 de diciembre de 2017). Lineamientos generales de protección de datos personales para el sector público. *Diario Oficial de la Federación*. Obtenido de <http://inicio.inai.org.mx/AcuerdosDelPle-no/ACT-PUB-19-12-2017.10.pdf>

INTERÉS LEGÍTIMO, PORTABILIDAD Y BLANQUEO, Informe 0195/2017 (Agencia Española de Protección de Datos 27 de julio de 2017).

LEY GENERAL DE SALUD. (2018). *Diario Oficial de la Federación*. México. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/pdf/142_241218.pdf

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES. (05 de julio de 2010). *Diario Oficial de la Federación*. México. Obtenido de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS. (2017 de enero de 2017). *Diario Oficial de la Federación*. Obtenido de <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>

PERSONAL DATA PROTECTION COMMISSION OF SINGAPORE. (2020). *Response to feedback on the public consultation on proposed data portability and data innovation provisions*.

SISTEMA NACIONAL DE TRANSPARENCIA, A. a. (12 de febrero de 2018). Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. *Diario Oficial de la Federación*. México. Obtenido de https://dof.gob.mx/nota_detalle.php?codigo=5512847&fecha=12/02/2018

Sitios web

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (16 de diciembre de 2018). *¿Qué es el derecho a la portabilidad?* Obtenido de Agencia Española de Protección de Datos: <https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-el-derecho-la-portabilidad>

CDC. (14 de septiembre de 2018). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. Obtenido de Centers for Disease Control and Prevention: <https://www.cdc.gov/phlp/publications/topic/hipaa.html>

CÉSAR MANUEL VALLARTA PAREDES. (25 de octubre de 2019). Módulo 5. Portabilidad de Datos Personales. *Canal de You Tube del INAI*. Recuperado el 19 de octubre de 2021, de <https://www.youtube.com/watch?v=3rVKwvIQrZU>

Comisión Europea. (16 de diciembre de 2018). *¿Qué es el derecho a la portabilidad?* Obtenido de Agencia Española de Protección de Datos: <https://www.aepd.es/es/documento/wp242rev01-annex-es.pdf>