Núm. 11, enero-junio de 2021

Revista

ESTUDIOS EN DERECHO A LA INFORMACIÓN

Universidad Nacional Autónoma de México
Instituto de Investigaciones Jurídicas
Facultad de Ciencias Políticas y Sociales
Instituto Nacional de Transparencia, Acceso
a la Información y Protección de Datos Personales
Centro de Investigación y Docencia Económicas

Revista Estudios en Derecho a la Información, núm. 11, enero-junio de 2021, es una publicación semestral editada por la Universidad Nacional Autónoma de México, Ciudad Universitaria, Coyoacán, 04510 Ciudad de México, a través del Instituto de Investigaciones Jurídicas, Circuito Maestro Mario de la Cueva s/n, Ciudad de la Investigación en Humanidades, Ciudad Universitaria, 04510 Ciudad de México, teléfono 5622 7474, correo electrónico: *redi.iij@unam.mx*. Editor responsable: Daniel Vázquez. Certificado de Reserva de Derechos al Uso Exclusivo del Título: 04-2016-021916284300-102. Certificado de Licitud de Título y Contenido: 17309. ISSN (versión electrónica): 2594-0082. ISSN (versión impresa): 2683-2083.

Jaime García Díaz
Cuidado de la edición y formación en computadora

Gilda Bautista Ravelo
Apoyo editorial

Ana Julieta García Vega
Diseño de interiores

Primera edición: 10 de diciembre de 2020

INSTITUTO DE INVESTIGACIONES JURÍDICAS

Circuito Maestro Mario de la Cueva s/n
Ciudad de la Investigación en Humanidades
Ciudad Universitaria, 04510 Ciudad de México

Impreso y hecho en México

ISSN (versión electrónica): 2594-0082
ISSN (versión impresa): 2683-2083

CONTENIDO

ARTÍCULOS

COMENTARIOS JURÍDICOS

RESEÑAS BIBLIOGRÁFICAS

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Artículos

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

LOS PERFILES DIGITALES DESPUÉS DE LA MUERTE, UNA PERSPECTIVA EUROPEA

DIGITAL PROFILES AFTER DEATH, A EUROPEAN PERSPECTIVE

*Diana Paola González Mendoza**

RESUMEN. Las nuevas tecnologías de la información y la comunicación y, específicamente, las redes sociales, generan un impacto directo en el desarrollo de la personalidad de la población mundial. Hasta junio de 2019, la red social *Facebook* contaba con dos mil millones de usuarios, lo que pone en evidencia la importancia que tiene en la actualidad la protección de nuestros datos en estas plataformas digitales. Sin embargo, ¿qué pasa con nuestras identidades digitales después de nuestra muerte? Esta comunicación pretende exponer el panorama actual nacional y europeo sobre el tema, tratando principalmente la ley catalana acerca de las voluntades digitales cuando ocurra fallecimiento o incapacidad (Ley 10/2017, del 27 de junio), así como otros desarrollos jurídicos en países de nuestro entorno, como Francia (Ley núm. 2016-1321 del 7 de octubre de 2016 para una República Digital) y Alemania (Sentencia del 31 de mayo del 2017 del Kammergericht, Berlin), que puedan servir de referencia para el tratamiento de esta cuestión en España. Simultáneamente, se valorarán las repercusiones que tiene el contenido digital de la persona fallecida en los derechos personalísimos de las personas vivas.

* Becaria del Programa de Ayudas Predoctorales "Severo Ochoa", Grupo de Investigación SPAG, Universidad de Oviedo. La beca se realiza gracias a las ayudas económicas de movilidad de excelencia para docentes e investigadores de la Universidad de Oviedo, 2019, financiadas por el Banco Santander, y a la colaboración del centro de destino: el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. *gonzalezdiana@uniovi.es*.

Fecha de recepción: 9 de diciembre de 2019.
Fecha de dictamen: 8 de marzo de 2020.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

PALABRAS CLAVE. Redes sociales, identidad digital, TIC, testamento digital.

ABSTRACT. New information and communication technologies and, specifically, social networks, generate a direct impact in the development of the personality of the World's population. Until June of the last year, the social network Facebook had two billion users, something that highlights the importance of protecting our personal data in these digital platforms. However, what happens with our digital identities after our death? The aim of these report is to present the national and European panorama on this matter, dealing mainly with the Catalonian law on digital wills in the case of death or disability (Law 10/2017, June 27th) as well as other legal developments in European countries such as France (Law num. 2016-1321 7th October 2016 for a Digital Republic) and Germany (sentence 31 st Mat 2017 of Kammergericht, Berlin), which may serve as a reference for the study of this issue in Spain. Simultaneously, the repercussion that the digital content of a deceased person in the personal rights of alive people will be assessed.

KEYWORDS. Social network, digital life, new information technologies, digital will.

I. Introducción

Indudablemente internet ha cambiado nuestras vidas, en la actualidad la principal forma de relacionarnos con otros se realiza a través de este medio, y en gran medida a través de las redes sociales, definidas como plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios, que comparten intereses comunes (GT 29, 2009). Este ciberespacio, como bien apunta Écija Bernal, constituye un nuevo mundo que no puede ser ajeno al derecho y a los distintos ordenamientos jurídicos (Écija Bernal, 2017). En abril de este año, el creador de la principal red social (*Facebook*) anunció en su página personal que dicha red contaba ya con dos mil millones de usuarios (Zuckerberg, 2019). Si tomamos en cuenta que esta red social fue creada en 2009, deducimos entonces que la mayoría de los usuarios son *millennials*, es decir, personas nacidas entre 1980 y 2000 (Burke, 2017: 5). Como consecuencia de lo anterior, los principales usua-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

rios de este tipo de medios aún no conciben la idea de la muerte a corto plazo. De acuerdo con el informe "Digital 2019", elaborado por la empresa *Hootsuite*, de los 4388 mil millones de personas que usan internet globalmente a diario, 3484 mil millones de personas tienen redes sociales, de los cuales casi el 60% están en la franja de edad comprendidos entre los 18-34 años (*Hootsuite*, 2019), quizás por ello este tipo de planteamientos aún no nos resultan familiares.

Durante nuestra vida digital somos creadores de perfiles de usuarios digitales en diversos servicios de la sociedad de la información, entre los que se encuentran las redes sociales, dentro de las cuales podemos generar diversos contenidos como fotografías, entradas a blogs, comentarios a diversas publicaciones, etc. También somos consumidores *on-line* en diversas plataformas, principalmente de películas, canciones, videojuegos, libros electrónicos, lo cual hace que debamos plantearnos la siguiente cuestión ¿qué es lo que pasa con nuestros perfiles en el ámbito digital cuando nuestra personalidad se ha extinguido?

II. Transmisión *mortis causa* de perfiles digitales

Tal y como establece el artículo 32 del Código Civil español (CC), la personalidad se extingue con nuestra muerte, por lo que todos los derechos personalísimos también. Éstos son, según Pascual Medrano, derechos derivados de la propia naturaleza humana, y destinados, justamente, a la protección integral de la persona (Pascual Medrano, 2003). Con relación a lo anterior, para hablar de una sucesión, siempre debemos tener claro cuáles son los bienes o derechos que tenía el causante al momento de su fallecimiento. Por consiguiente, ¿cuáles serían los bienes en el mundo digital que se pueden transmitir a la muerte del individuo?

Como es bien sabido, los bienes pueden ser tangibles (o materiales) e intangibles (o inmateriales). Los primeros son prácticamente inexistentes en el plano digital; los segundos, en sentido amplio, son todos aquellos que carecen de corporeidad o bien los que, además, no se pueden percibir mediante el sentido del tacto (con lo que excluimos de esta categoría a las energías) o acaso, a través de cualesquiera de los sentidos corporales (Lacruz Berdejo, 2008), y están basados en la creación artística, científica o literaria. Éstos pueden ser explotados económicamente si el titular lo desease, así como disponer de ellos cumpliendo con las formalidades exi-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

gidas en la ley,[1] e indudablemente este tipo de propiedad tiene cabida en el plano digital.

Sin embargo, León Robayo defiende una tercera categoría a la que él denomina como virtuales, para el autor es una categoría intermedia entre las dos anteriores, pero con características propias. En ella se involucran elementos intelectuales que son perceptibles por los sentidos, especialmente la vista y, en algunos casos, a través de comandos de voz. Estos elementos informáticos son puestos en funcionamiento por la interacción que el individuo ejerce directa o indirectamente sobre ellos (León Robayo, 2006).

Es en la web donde tienen cabida los perfiles de los usuarios. Éstos no pueden ser considerados de manera estricta como un bien inmaterial ante su falta de explotación y disposición. El contenido de estos perfiles puede afectar a derechos fundamentales personalísimos como es el derecho a la protección de datos personales, el derecho al honor, el derecho a la intimidad personal y familiar, así como el derecho a la propia imagen, todos ellos contenidos en el artículo 18 de la Constitución Española, así como su estrecha relación con el respeto a la dignidad de la persona, al margen de las creaciones *on-line*. Estos perfiles tienen relación con la denominada "identidad digital", la cual ha sido definida por González Granado como un derecho de la personalidad autónomo (conceptualmente diferenciado del honor, la propia imagen, el nombre o los apellidos) y, como tal, innato, *erga omnes*, privado, irrenunciable y extrapatrimonial (aun cuando en sus manifestaciones sea susceptible de valoración económica y de negocios jurídicos) (González Granado, 2016). Es decir, que la identidad digital consiste en trasladar nuestra identidad analógica al entorno digital o, mejor dicho, trasladar la percepción de nosotros mismos junto con nuestra imagen a nuestros perfiles digitales.

Sin embargo, nuestra identidad digital personal no sólo está conformada por nuestra percepción propia, tal y como sucede en un entorno analógico, también está configurada por la que se nos da en un entorno "oficial". Esta identidad es definida a partir de las circunstancias y del entorno público y recognoscible de cada persona (Piñar Mañas, 2018). Puede llegar a ser definida no desde la autonomía de la persona sino de manera heterónoma (Piñar Mañas, 2019), sobre todo por el uso de nuevas tecnologías.

[1] Los artículos 428 y 429 del CC regulan la propiedad intelectual, encuadrándola en la categoría de propiedades especiales (título IV, capítulo III); otra norma que se encarga principalmente de su regulación es la Ley de Propiedad Intelectual (Real Decreto Legislativo 1/1996, del 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Por ejemplo, en la publicidad en línea se utilizan distintos tipos de *cookies* que junto con la dirección IP pueden arrojar un perfil detallado de las preferencias de las personas; a este tipo de publicidad se le conoce como publicidad comportamental u *Online Behavioural Advertising*.

Entonces, ¿podríamos heredar nuestros perfiles digitales? Éstos están asociados principalmente al nombre y a la imagen del usuario, y la mayoría de veces, al hacer un perfil público en las redes sociales, se pierde parte de nuestra intimidad familiar y personal. Además de quedar expuestos a cualquier intromisión a nuestro honor, a la propia imagen, se puede también vulnerar el derecho a la protección de datos por la cantidad de información que vamos aportando sobre nosotros mismos o por terceros cuando se nos etiqueta en alguna publicación o fotografía. A partir de esta información se puede perfectamente elaborar un perfil ideológico, social y político dentro de las redes sociales con base en los *likes* o *retweets*. Es por ello que, al ser parte de la expresión más personal de los usuarios, se evidencia que la respuesta al planteamiento anterior es negativa. Con relación a esto, González Granado cree que la identidad digital es un concepto ligado a la personalidad del sujeto, y una vez fallecido como ocurre con los restantes atributos de la personalidad, sus blogs, perfiles en redes sociales, sus *nicks* en comunidades virtuales pasan a integrar la *memoria defuncti* a modo de identidad digital *post mortem* (González Granado, 2016).

Está claro que nuestros perfiles digitales no se pueden transmitir por causa de muerte, debido a su carácter instrumental, tanto en la proyección de derechos como para ser sujetos de obligaciones en el ámbito digital. Entonces ¿cabría la posibilidad de decidir qué hacer con nuestros perfiles en redes sociales después de nuestra muerte? ¿podríamos incorporar en nuestro testamento nuestra voluntad en el plano digital? Antes de contestar a estas preguntas no debemos olvidar que los contenidos que generamos dentro de nuestros perfiles sí que pueden llegar a ser considerados como bienes inmateriales susceptibles de explotación (fotografías, vídeos, opiniones, etcétera) y, por lo tanto, susceptibles de contemplarse en un testamento.

Ahora bien, los perfiles de las personas, en los denominados servicios de red social (SRS), tienen múltiples perspectivas: por una parte, pueden ser el medio para disponer de los bienes inmateriales contenidos en éstos, aunque después de la muerte de la persona éstos pueden convertirse en una fuente de protección gracias a la *memoria defuncti*, sólo en caso de cuentas conmemorativas y, por otro lado, las identidades digitales deberían de ser susceptibles de eliminación tras la muerte de su titular o en su caso, que los otorgantes de un testamento puedan prever qué hacer con éstos tras su muerte.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Como sabemos, el testamento es el instrumento ideal para plasmar la última voluntad de las personas. Con la aparición de las nuevas tecnologías surge también el término de "testamento digital" que, como bien apunta Llopis Benlloch, puede generar una serie de confusiones, ya que las personas pueden referirse a éste como el instrumento que incluye previsiones para la herencia digital de la persona como perfiles en redes sociales, archivos de audio y video, etcétera, o al testamento que se hace *online* por internet (Llopis Benlloch, 2016). En esta comunicación sólo nos referimos al instrumento donde constan las últimas voluntades de las personas.

De modo que, ¿los testamentos pueden contener disposiciones de lo qué debe hacerse con la huella digital del otorgante? En principio diríamos que sí, al menos en lo que se refiere a la eliminación de la cuenta o a su conversión en conmemorativa en las redes sociales. En la actualidad, la Ley Orgánica 3/2018, del 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), prevé en su artículo 96 el derecho al testamento digital, el cual se estudiará de manera posterior en este artículo.

En cuanto a las disposiciones civiles, para el testamento abierto a nivel nacional se prevén ciertas formalidades del acto de otorgamiento: deberán de concurrir dos testigos instrumentales (artículo 698 del CC); el notario, en presencia de éstos, realizará una lectura testamentaria (artículo 699 del CC), y deberá de constar en escritura pública (artículo 704 del CC). De conformidad con el artículo 17.1, cuarto párrafo, de la Ley del Notariado, los otorgantes tienen derecho a obtener primera copia de la escritura matriz. Hasta aquí parece que no tenemos mayor problema en incluir en el testamento este tipo de disposiciones, indicando específicamente las cuentas y/o usuarios en las diferentes redes sociales o en su caso de correo electrónico, encomendándole al albacea de la sucesión, a los herederos o a un legatario específico la supresión de dichos perfiles. Al no tratarse de disposiciones relativas de lo que debe de hacerse con restos tangibles, puede ser una medida eficaz, debido al tiempo que tienen los herederos para conocer el contenido del testamento (Reglamento de la Organización y Régimen del Notariado, 1944).

III. Acerca de los prestadores de servicios de la sociedad de la información

Son prestadores de servicios de la sociedad de la información aquellas personas físicas o jurídicas que proporcionan servicios de la sociedad de la

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

información (LSSI, 2002). Estos últimos son definidos como: "aquellos prestados a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario" (artículo 1.1.b) de la Directiva 2015/1535 del Parlamento Europeo y del Consejo, del 9 de septiembre de 2015, por la que se Establece un Procedimiento de Información en Materia de Reglamentaciones Técnicas y de Reglas a los Servicios de la Sociedad de la Información —versión codificada—). En España, la Ley 34/2002, del 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, también prevé como servicios de la sociedad de la información a los no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Así pues, *Facebook*, *Twitter*, *Instagram* o *LinkedIn*, de forma amplia, son prestadores de servicios de la sociedad de la información, y de manera específica, son SRS, ya que son plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes (GT 29, 2009). En cuanto a *Google* y *Yahoo!*, también de forma amplia son prestadores de servicios de la sociedad de la información, aunque, debido a los diversos servicios que prestan como correo electrónico, servicio de red social, almacenamiento y edición de fotografías, también merecen ser vistos desde distintas perspectivas. No obstante, en esta comunicación sólo se analizarán como proveedores de correo electrónico. Todos estos proveedores no están establecidos en territorio de la Unión, la mayoría de ellos tienen su sede principal en Estados Unidos, aunque esta circunstancia no impide que les sea de aplicación la normativa española, ya que dirigen sus servicios específicamente al territorio español y a usuarios españoles, mediante un establecimiento permanente situado en España (LSSI, 2002), o dentro de la Unión Europea; por ejemplo, en el caso de *Google LLC*, su sede para el cumplimiento de la normativa en materia de protección de datos está en Irlanda desde 2017.

La importancia de los prestadores de servicios radica en la velocidad en que desarrollan, crean e implementan nuevos servicios o posibilidades en sus plataformas digitales. Conforme a esto, la mayoría de las veces la realidad sobrepasa al contenido de las normas jurídicas, y es por ello que hasta hace poco sus usuarios tenían que atenerse a lo que éstos establecieran en sus políticas de uso para mitigar este tipo de circunstancias. Pero, ¿los prestadores de servicios de la sociedad de la información contemplan o tienen habilitada alguna forma para que el albacea o herederos de los usuarios tras su muerte puedan eliminar sus cuentas?

Facebook tiene habilitado un formulario de "Solicitud especial para la cuenta de una persona fallecida o incapacitada" (*Facebook*, 2019), cuyo

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

objeto es la eliminación de cuentas de personas con incapacidad médica que ha fallecido, o bien para enviar solicitudes especiales de cuentas conmemorativas. Se indica en el mismo que no se proporcionará a nadie la información del inicio de sesión de ninguna cuenta perteneciente a un usuario fallecido. Para el caso de personas fallecidas, el peticionario en su solicitud de eliminación tiene que proporcionar su nombre completo, además de los siguientes datos de la persona fallecida: el nombre completo que aparece en la cuenta, la dirección web (URL) de la biografía y el correo electrónico asociado al perfil. Para hacerla conmemorativa se tienen que cubrir los anteriores requisitos, además se deberá de proporcionar una copia o foto del obituario, certificado de defunción, esquela que contenga la fecha del fallecimiento.

Instagram, al pertenecer a *Facebook* desde el 2012 (*Instagram*, 2012), también cuenta con la opción de informar del fallecimiento del titular de una cuenta y con ello convertir la cuenta del fallecido en conmemorativa. Para ello se deberá cumplimentar un formulario específico (*Instagram*) que es prácticamente idéntico al de *Facebook*, con la salvedad de que éste requiere del solicitante una prueba del fallecimiento del titular de la cuenta. En caso de que sean los familiares directos quienes soliciten la eliminación, deberán de aportar algún documento que pruebe la muerte del titular.

Por su parte, *Twitter* tiene habilitado un "formulario de privacidad" (*Twitter*), para solicitar la desactivación de la cuenta de un usuario fallecido o incapacitado. Los datos por proporcionar, en caso de solicitar la desactivación de la cuenta por fallecimiento, serían: el nombre de usuario, nombre completo del titular, la relación de parentesco del peticionario, así como el nombre completo de este último, y su correo electrónico. En esta página se indica que, después de enviar este formulario, el peticionario recibirá instrucciones adicionales.

LinkedIn dispone también de un formulario para la eliminación de la cuenta de un usuario fallecido (*LinkedIn*). Los datos por rellenar son los mismos, pero con la especificidad del deber de proporcionar un enlace electrónico a un obituario o esquela, así como indicar cuál fue la última empresa en donde trabajó el fallecido.

Yahoo! no tiene un formulario, como los demás prestadores de servicios mencionados anteriormente; en este caso, su página de ayuda indica que se tiene que poner en contacto con el equipo de atención al cliente para obtener ayuda con el cierre de la cuenta. También se indican los documentos que deberán ser aportados para poder procesar este tipo de solicitud, entre ellos una carta con la solicitud y el ID de *Yahoo!* del fallecido, una

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

copia de un documento que nombre al solicitante como representante legal o testamentario del fallecido, y una copia del certificado de defunción del titular de la cuenta de *Yahoo!*

En el caso de *Google*, además de contar con la posibilidad de hacer una solicitud relacionada con la cuenta de una persona fallecida aportando el nombre del usuario, una fotocopia del DNI y certificado de defunción (*Google*), se proporciona la posibilidad a los usuarios de planificar qué ocurrirá con la cuenta en caso de fallecimiento o inactividad en *Google* (*Google*), pudiendo escoger entre cuatro periodos de inactividad disponibles (3, 6, 12 y 18 meses), y debiendo proporcionar de manera obligatoria un número telefónico. El paso siguiente es la elección de la persona o personas (hasta 10) a notificar en caso de que la cuenta esté inactiva por el periodo previamente indicado, debiendo de señalar su teléfono y el contenido al que podrá tener acceso por medio de una descarga después del fallecimiento. Por último, se pregunta al usuario si desea eliminar la cuenta y el contenido cuando ésta se vuelva inactiva. El contenido de la cuenta podrá ser descargado, por la o las personas designadas al efecto, tres meses antes de que se cumpla la fecha de inactividad elegida. Después de todos estos pasos se permite revisar el plan de inactividad para confirmarlo, y activar la opción de recibir recordatorios por correo electrónico cuando se active el administrador de cuentas inactivas.

IV. Los remedios jurídicos a la problemática actual en Europa. Especial mención al caso español

La defensa de la *memoria defuncti* (Alonso Pérez, 2003) está prevista en la Ley Orgánica 1/1982, del 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen. Como bien apunta Bodas Daga, la LO 1/1982 nace con la finalidad de proteger civilmente estos derechos y cuyo objeto de protección es la memoria del difunto (Bodas Daga, 2007: 152). En el artículo cuarto de esta ley se establece la posibilidad de que el otorgante de un testamento pueda designar a una persona para el ejercicio de las acciones de protección civil de estos derechos tras su muerte. En caso de no haberse establecido por disposición testamentaria, estarán legitimados el cónyuge, los descendientes, los ascendientes y hermanos de la persona afectada que vivan al tiempo de su fallecimiento (LO 1/1982). De no existir alguna de ellas, al momento de la muerte del causante, el Ministerio Fiscal será el legitimado para el ejercicio de estas acciones, siempre que no hayan transcurrido 80 años desde el fallecimiento

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

del afectado (LO 1/1982). Incluso las personas legitimadas podrán continuar la acción ya entablada por el titular del derecho lesionado, si falleciere o aun cuando la lesión a uno de estos derechos se haya producido en vida, y el titular del derecho lesionado fallezca sin haber podido ejercitar por sí o por su representante legal las acciones previstas en esta ley (LO 1/1982).

A nivel nacional, hasta hace poco no existía ninguna ley que previera el destino de lo que hoy conocemos como huella digital tras la muerte, ni tampoco de manera específica si las personas podían incluir en su testamento o cualquier otro tipo de documento su última voluntad en materia digital, situación que ha cambiado desde el 2017. El jueves 29 de junio de 2017 se publicó en el *Diario Oficial de la Generalitat de Cataluña*, la Ley 10/2017, del 27 de junio, de las Voluntades Digitales y de Modificación de los Libros Segundo y Cuarto del Código Civil de Cataluña, la cual busca establecer normas que permitan determinar cómo se debe administrar el legado relativo a la actividad de cada persona en los entornos digitales ante la muerte (Ley 10/2017, del 27 de junio).

En este artículo sólo se tratarán los cambios introducidos en el Libro Cuarto del Código Civil de Cataluña (sucesiones). Esta ley modifica el artículo 421-2, relativo al contenido del testamento (artículo 7o. de la Ley 10/2017) y el apartado primero del artículo 428-1 relativo al modo sucesorio (artículo 9o. de la Ley 10/2017). Añade el artículo 411-10 relativo a las voluntades digitales en caso de muerte (artículo 6o. de la Ley 10/2017); el artículo 421-24 relativo a la designación de la persona encargada de ejecutar las voluntades digitales (artículo 8o. de la Ley 10/2017); la disposición adicional tercera, relativa a la creación del registro electrónico de voluntades digitales (artículo 10 de la Ley 10/2017) y la disposición final quinta, relativa a la organización, funcionamiento, y acceso al registro electrónico de voluntades digitales (artículo 11 de la Ley 10/2017).

Con esta reforma se abre la posibilidad a que las personas con vecindad catalana puedan disponer qué hacer con sus cuentas de los servicios de la sociedad de la información tras su muerte. En estas disposiciones se prevé que la ejecución de las voluntades digitales estará a cargo de herederos, el albacea o cualquier persona que se haya designado específicamente para ello. La persona designada para ejecutar la voluntad digital del fallecido podrá informar del fallecimiento del *de cujus* a los prestadores de servicios de la sociedad de la información, solicitar la cancelación de las cuentas activas del fallecido, solicitar a los prestadores de los servicios ceñirse a lo establecido en sus cláusulas contractuales o que se adopten las medidas que tengan previstas en el momento de fallecimiento del usuario y, en su caso, que se les sea entregada una copia de los archivos digita-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

les del fallecido si procede (artículo 6o. de la Ley 10 /2017). Esta última posibilidad podría acarrear problemas en el futuro por la posible colisión con el derecho al secreto de las comunicaciones (artículo 18.3 de la CE), sobre todo por el contenido de los correos electrónicos, e incluso podría colisionar con otros derechos de la personalidad contenidos en el mismo precepto (artículo 18 de la CE), como la imagen y la intimidad personal o familiar de las personas si los prestadores de servicios autorizasen la entrega de fotos que contengan imágenes de terceros o donde aparezcan éstos.

Otra cuestión que tiene que ver con el contenido de los derechos de la personalidad es la falta de disposición expresa del causante para tener acceso a sus cuentas y archivos. En principio no se podrá dar acceso a la cuenta ni descargar el contenido del causante a menos de que haya una autorización prevista al heredero o albacea universal a esos efectos (artículo 6o. de la Ley 10/2017). En este caso, también tendría que ponderarse si debe de prevalecer la última voluntad del *de cujus* o los derechos de las de personas vivas (imagen, intimidad personal o familiar y secreto de las comunicaciones contenidos en el artículo 18 de la CE) con las que compartía, por este medio, contenido electrónico.

El testamento, codicilo y las memorias testamentarias, es decir, las tradicionales disposiciones de última voluntad en Cataluña, son también medios válidos en derecho por los cuales las personas pueden plasmar sus voluntades digitales. Y con motivo de la Ley 10/2017, las personas incluidas en su ámbito de aplicación también pueden realizar un documento específico donde se señale qué se deberá hacer con sus cuentas en el ámbito digital. Dicho documento no produce efectos si existen disposiciones de última voluntad, y tendría que inscribirse en el registro electrónico de voluntades digitales (también de nueva creación en base a lo establecido en la Ley 10/2017). Según esta Ley, en caso de no existir cualquier documento enumerado en el principio de este párrafo, el heredero o albacea universal puede realizar cualquiera de las tres acciones de disposición, de acuerdo con los contratos que el causante haya suscrito con los prestadores de servicios digitales o de acuerdo con las políticas que estos prestadores tengan en vigor. Lo anterior, no es más que la positivización de una realidad que ya se da en la práctica para las personas que se ven inmersas en esta situación, pues dependen de las políticas de uso que tengan implementadas los prestadores de servicios al momento de su muerte.

Los artículos 10 y 11 de la Ley 10/2017 prevén la creación de un registro al que podrán tener acceso las personas que deseen registrar sus voluntades digitales. Una vez muerto el autor de estas voluntades, tendrán acceso a este documento aquellas personas que demuestren un interés

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

legítimo o sean las designadas por el autor para la ejecución de esas voluntades digitales. Es posible que el legislador catalán en este aspecto se haya extralimitado debido a que no tiene competencias para la creación de registros (artículo 149.1.8a. de la CE). También se abre la posibilidad de someter a mediación cualquier controversia que surja de la aplicación de la ley y, se prevé el desarrollo reglamentario de estas disposiciones.

Esta ley fue impugnada por el gobierno de la nación con relación a diversos preceptos entre los que se encuentran las disposiciones por las que se modifican o introducen cambios al Libro Cuarto del Código Civil de Cataluña, específicamente los artículos 6o., 8o., 10, 11 y D. F. 1a. Este recurso tiene fundamento exclusivamente competencial en cuanto a la creación del registro electrónico de voluntades digitales (STC 7/2019). Como se ha señalado anteriormente, la competencia de creación de registros públicos es de carácter estatal, de acuerdo con el artículo 149.1.8a., CE.

La Sentencia que resuelve este recurso realiza un análisis competencial sobre la creación de este registro. Cataluña cuenta con la competencia ejecutiva en materia de registros (STC 103/1999, FJ 4), de acuerdo con el artículo 147.3 del Estatuto de Autonomía de Cataluña, y para la creación de registros administrativos ligados a una competencia propia (SSTC 32/1983, del 28 de abril y 87/1985, del 16 de julio). El Tribunal Constitucional entiende que, en este caso, se pretende la creación de un registro público de derecho privado, en el que han de inscribirse para su validez los documentos de voluntades digitales, en defecto de disposiciones de última voluntad (STC 7/2019, F.D.4) y con ello, se invade la competencia exclusiva del Estado de creación de registros públicos en el ámbito civil. Por tanto, se declara inconstitucional el artículo 10 de la referida ley. Y como consecuencia de ello también se declara inconstitucional el contenido del artículo 11 por el que establecía su organización, funcionamiento y acceso. También se declaran parcialmente inconstitucionales por conexión los artículos 6o. y 8o., en lo relativo al documento de últimas voluntades digitales.

La sentencia cuenta con un voto particular. La magistrada formulante considera que no se trata de un registro de carácter civil, sino de carácter administrativo, tal y como reconoce la norma en su preámbulo. Este voto particular pivota sobre cuatro razones, en las que se fundamenta para disentir del fallo del pleno del TC. La primera de ellas es que la inscripción del documento de voluntades digitales no determina ni la naturaleza jurídico-civil de tales disposiciones, ni la naturaleza del propio registro (voto particular Rec. 4751-2017, núm. 2). Por una parte, la inscripción constituye un deber, mas no una obligación que condicione su validez; la norma

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

tampoco establece nada al respecto, más bien sería una garantía de seguridad para los interesados (voto particular Rec. 4751-2017, núm. 2) como sucede con los instrumentos ológrafos, los que tienen plena eficacia pese a su falta de inscripción, por tanto, que se pueda registrar no determina que sea un acto de naturaleza civil. El segundo de los fundamentos que se hace valer en este voto particular es que no todos los actos que adquieren eficacia a la muerte de una persona entran en la categoría del derecho de sucesiones (voto particular Rec. 4751-2017, núm. 3), como ejemplo más evidente se cita el registro de parejas estables, el cual afecta de manera obvia al estado civil de la persona y con vigencia incluso *post mortem*, pero no compete a la sucesión de ésta; son registros además de naturaleza administrativa (voto particular Rec. 4751-2017, núm. 3). La tercera razón que se esgrime es que la sentencia parte de la idea de que las voluntades digitales son actos de disposición respecto al patrimonio digital de la persona y por ello el contenido de este documento es de naturaleza civil; no obstante, en el voto particular se resalta el hecho de que ni siquiera el registro de actos de última voluntad tiene naturaleza civil a efectos del artículo 149.1. 8a., CE (voto particular Rec. 4751-2017, núm. 4), pues sólo publicita la existencia o inexistencia de tal documento, y de ningún modo tiene efectos declarativos de derechos subjetivos ni los reconoce, y tampoco existe una función calificadora de algún registrador que lleve a cabo un control de legalidad, por lo tanto, puede ser válida la naturaleza administrativa de tal registro. Y el último de los argumentos consiste en subrayar que, en realidad, lo que recoge el documento es la voluntad del fallecido respecto a la realización de actividades muy concretas, que están directamente relacionadas con el ejercicio de derechos personalísimos de carácter no patrimonial, por tanto, no transmisibles *mortis causa*, como las de comunicar a los prestadores de servicios digitales su defunción; solicitar la cancelación de las cuentas activas, que ejecuten las cláusulas contractuales o que se activen las políticas establecidas para los casos de defunción y, en su caso, que liberen una copia de los archivos digitales que estén en sus servidores (voto particular Rec. 4751-2017, núm. 5).

Se debe de estar de acuerdo, de manera parcial (casi total), con este voto particular, por coherencia con lo que se ha defendido y determinado a lo largo de este artículo. Específicamente por el carácter instrumental de los perfiles para el ejercicio de derechos y obligaciones en el ámbito digital, en cuanto proyectan los elementos personalísimos como la identidad, nuestra imagen, nuestros datos personales, e incluso nuestra libertad de expresión e información, de manera colateral permiten a otros individuos el pleno goce y ejercicio de sus derechos, determinada en forma de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

obligación. No se puede estar totalmente de acuerdo con la parte sobre disposición de los archivos del difunto, puesto que, como se expondrá de manera posterior, podría acarrear problemas, ya que en este contenido podría haber imágenes, publicaciones o cualquier bien intangible, susceptible de explotación, que no sea de su propiedad. Además de que el uso del material en tenencia del difunto puede acarrear violaciones a derechos personalísimos de personas aún vivas, pensemos en la propagación de una imagen compartida y publicada sin consentimiento, alguna republicación de autoría del difunto que lesione el honor de otra persona, e incluso el secreto a las comunicaciones por las conversaciones mantenidas por terceros con el difunto, etcétera.

El 6 de diciembre de 2018 fue publicada en el *Boletín Oficial del Estado* español la nueva LOPDGDD. En su artículo 3o. prevé lo relativo a los datos de las personas fallecidas, y en su artículo 96, lo relativo al testamento digital. Primeramente, se tiene que señalar que el considerando 27 del Reglamento (UE) 216/679 del 27 de abril de 2016, o también denominado Reglamento General de Protección de Datos, excluye su aplicación a los datos de las personas fallecidas, y son los Estados miembros quienes ostentan la competencia para legislar en este caso. Ahora bien, el artículo 3o. de la LOPDGDD faculta a las personas vinculadas, por razones familiares o de hecho (lo cual no excluye su ejercicio por parte de la pareja de hecho *supérstite*) y a los herederos, para que éstos puedan dirigirse tanto al responsable del tratamiento como al encargado para poder acceder, cancelar o suprimir los datos de la persona fallecida. En el caso del acceso, éste puede ser restringido si existiese una prohibición expresa por la persona fallecida o esté establecido así por ley. Las facultades antes señaladas también podrán ser ejercidas por representantes legales y por el Ministerio Fiscal cuando se trate de menores o personas con discapacidad (apartados 2 y 3 del artículo 3o. de la LOPDGDD).

El artículo 96 de la LOPDGDD, bajo el título de "Derecho al testamento digital", no se refiere propia y estrictamente a lo que es un testamento. Porque en un testamento se plasman las últimas voluntades de las personas; pero este artículo, en su apartado primero, determina la facultad de acceder a los datos por personas vinculadas por razones familiares o de hecho, a los herederos, y en el caso de menores y personas con discapacidad a sus representantes legales o en su caso al Ministerio Fiscal frente a los servicios de la sociedad de la información, siempre y cuando no hubiese una prohibición expresa para tal efecto o se establezca así en la ley. En la segunda parte de este artículo, se determina la facultad de las personas mencionadas anteriormente para decidir qué hacer con el perfil del finado,

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

bien mantenerlos o eliminarlos específicamente en redes sociales o equivalentes, a menos de que el fallecido haya determinado qué hacer con los mismos. Debe de entenderse equivalente en este contexto a todo servicio de la sociedad de la información que permita el mantenimiento y creación de algún perfil para tener acceso a éste. Sin embargo, en ambos casos se remite a una norma de carácter reglamentario aun inexistente, donde deban de preverse los requisitos, las condiciones para acreditar la validez y vigencia de los mandatos e instrucciones, y en su caso el registro de los mismos, que podría ser el mismo que se prevé en el artículo 3o. de esta ley orgánica (artículo 96.3 de la LOPDGDD).

En lo referente al marco europeo, Francia es uno de los países precursores en legislar el entorno digital, el 9 de diciembre de 2015 fue presentada ante la Asamblea Nacional el Proyecto de Ley para la República Digital (Project de Loi pour une République Numérique, 2015). Dentro de sus objetivos, se encuentra la introducción de nuevos derechos para las personas en el mundo digital, en materia de datos personales y acceso a los servicios digitales. La Loi no. 2016-1321 du 7 de Octobre 2016 pour une République Numérique fue llevada a cabo mediante el procedimiento acelerado de creación de normas francés, y vio la luz hasta el 8 de octubre de 2016 mediante su publicación en el *Diario Oficial* núm. 235. Se compone de 113 artículos, divididos en cuatro títulos, que versan fundamentalmente sobre conceptos ya ampliamente conocidos como *open data*, *open access*, integración de datos y la reutilización de información del sector público (Boto Álvarez, 2017).

Esta Ley modifica y actualiza diversas leyes adaptándolas al ámbito digital y tecnológico. Es de especial interés para este artículo el contenido de su artículo 63 por el cual se añade el artículo 40-1 a la Ley núm. 78-17 del 6 de enero de 1978 sobre la informática, archivos y libertades. Este artículo prevé que toda persona puede definir directrices relativas a la conservación, eliminación y comunicación de sus datos de carácter personal tras su fallecimiento (*Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès* —Loi no. 2016-1321 du 7 de Octobre pour une République Numérique—). Estas directrices pueden ser generales o particulares, en el primer caso comprenden la totalidad de los datos de carácter personal de la persona y deberán de estar inscritas en un registro único; en cambio, las directrices particulares se refieren a una parte de sus datos de carácter personal, y deberán de ser registradas por los prestadores de servicios a la información sin que sean unilaterales; es decir, para su validez requieren la previa aceptación del titular de los datos

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

personales. Además, toda cláusula contractual de condiciones generales de utilización de un tratamiento, que lleve datos de carácter personal y limite las prerrogativas reconocidas a una persona, en virtud del presente artículo se considera no escrito (*Toute clause contractuelle des conditions générales d'utilisation d'un traitement portant sur des données à caractère personnel limitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite* —Loi no. 2016-1321 du 7 de Octobre pour une République Numérique—).

Las personas que establezcan directrices de manera general podrán designar a una persona para que las ejecute después de su muerte. Sin embargo, una de las aportaciones más relevantes de esta ley consiste en establecer qué deberá de hacerse en caso de que la persona designada también haya fallecido, a falta de indicación o directriz en contrario, en caso de muerte de la persona designada, sus herederos tienen capacidad para tomar conocimiento de las directrices a la muerte de su autor y solicitar su puesta en marcha a los responsables de tratamiento concernidos (*A défaut de désignation ou, sauf directive contraire, en cas de décès de la personne désignée, ses héritiers ont qualité pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés* —Loi no. 2016-1321 du 7 de Octobre pour une République Numérique—).

En caso de ausencia de estas directrices, tras la muerte del individuo, los herederos pueden informar a los responsables del tratamiento de su fallecimiento. Como tal, los herederos pueden hacer que se proceda al cierre de las cuentas del difunto, oponerse a la continuación del tratamiento de datos de carácter personal que le conciernan o que sean puestos al día (*A ce titre, les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour* —Loi no. 2016-1321 du 7 de Octobre pour une République Numérique—). Con respecto a esto, el prestador de servicios tiene la obligación, derivada de esta petición, de justificar que se ha procedido, ya sea al cierre de la cuenta o que se han dejado de tratar los datos de esa persona. La misma ley establece la obligación que tienen los prestadores de servicios de mantener informado al usuario del tipo de datos que serán afectados a su muerte y le permitirá elegir si comunicar o no sus datos a un tercero que él designe (*Tout prestataire d'un service de communication au public en ligne informe l'utilisateur du sort des données qui le concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne* —Loi no. 2016-1321 du 7 de Octobre pour une République Numérique—).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

La aportación en el ámbito jurídico de Alemania no es una ley, sino una sentencia, que nos puede dejar entrever las cuestiones prácticas ante la falta de legislación aplicable específica en la materia a este supuesto. La sentencia es del 31 de mayo de 2017, procedente de la Corte de Apelación de Berlín (Kammergericht, Berlin, 2017). Resumidamente, esta sentencia resuelve una cuestión originada por el fallecimiento de una niña de 15 años, bajo causas aún no esclarecidas. Cabe destacar que esta niña, a la que denominaremos "L", un año antes de tener 14 años se hizo un perfil en la red social *Facebook*. A su muerte, su madre esperaba obtener a través de la cuenta de *Facebook* de su hija, cualquier indicio de posibles intenciones o motivos en caso de que la muerte de la fallecida fuera un suicidio (*über den Facebook-Account ihrer Tochter etwaige Hinweise über mögliche Absichten oder Motive ihrer Tochter für den Fall zu erhalten, dass es sich bei dem Tod der Erblasserin um einen Suizid handele*). Sin embargo, no pudo acceder al contenido del usuario debido a que previamente había dado parte de este hecho a la red social y convertido en conmemorativo su perfil.

En primera instancia el Tribunal Regional de Berlín (Landgericht, Berlin) condenó a *Facebook* a permitir el acceso a la cuenta y el contenido de "L" por la aplicación del artículo 1922 del Código Civil alemán (BGB), pues entendía que el prestador de servicios con el que tenía el contrato "L", a su muerte colocaba a los herederos de ésta en una situación de sustitución por la heredabilidad de la relación contractual, aun cuando no lo estableciesen así las condiciones de uso del prestador de servicios.

Facebook, por su parte, recurrió esta decisión, cuyo argumento principal estaba basado en la refutación de la valoración de la cuestión de la heredabilidad de las cuentas, pues el tribunal *a quo* no consideró el contenido del secreto de las telecomunicaciones establecido en el artículo 10 de la Ley Fundamental alemana. Y otras cuestiones relativas a la naturaleza de la relación contractual con sus usuarios, la extinción del papel de guardián de la privacidad que tienen los padres para con sus hijos y su extinción por causa de muerte (artículo 1623 de la BGB), la autodeterminación de las personas, así como la intención real de las partes en el contrato, llevado a cabo entre *Facebook* y sus usuarios, especialmente, cuando estos últimos conocen la condición personalísima del servicio; por tanto, en ningún momento consienten el acceso a sus cuentas después de su fallecimiento. La Sala de Apelación resuelve que efectivamente no se tomó en consideración por el tribunal *a quo* lo establecido en el artículo 7o. de la Carta de Derechos Fundamentales de la Unión Europea, el cual establece que: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones" (CDFUE, 2000), ni

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

el contenido del artículo 10 de la Ley Fundamental alemana el cual determina que: "(1) El secreto epistolar, así como el secreto postal y de las telecomunicaciones son inviolables. (2) Las restricciones sólo podrán ser ordenadas en virtud de una ley" (Ley Fundamental alemana). También se determina en la sentencia que los contenidos de los mensajes son privados y que, al no estar involucrados los herederos en esas comunicaciones, no pueden tener acceso, ni el proveedor puede darle acceso a éstos debido al papel de guardián de la comunicación que ostenta en las comunicaciones electrónicas. Es más, se determina que la usuaria fallecida tampoco dio su consentimiento para que se llevase a cabo la trasferencia del contenido de sus comunicaciones, situación que por sí misma la fallecida tampoco asumió que se realizaría después de su muerte, ni mucho menos los demás usuarios con los que se relacionaba por esta red social.

El tribunal *ad quem* establece que los usuarios o perfiles no son heredables debido al contenido de datos contenidos en ellos, pues el derecho de autodeterminación informativa y el de protección de datos personales se extinguen con la muerte, situación determinada por su carácter personalísimo, es por ello que los herederos no son capaces de ejercer derechos de esa naturaleza o relacionados con el contenido de los mismos. Esta sentencia es de gran relevancia, debido a que resuelve problemas prácticos por analogía de las normas jurídicas en materia de sucesiones, a falta de una norma específica aplicable al momento de su emisión.

El 12 de julio de 2018, el Tribunal Federal de Justicia Alemán (Bundesgerichtshof, 2018) dictó sentencia en última instancia sobre este asunto, por haberse interpuesto un recurso en contra de la determinación del *ad quem*. Esta sentencia merece ser objeto de un estudio particular; sin embargo, a grandes rasgos este Tribunal asemeja la comunicación electrónica con la analógica, entiende que los padres de la menor tienen derecho al acceso a la cuenta de *Facebook* como consecuencia de la sustitución por heredabilidad de la misma y, por lo tanto, se debe de entender a éstos como los nuevos titulares, en concordancia con la Sentencia de Primera instancia, núms. 38, 50, 53, 54, 60, 63, 72, 78, 85, 93 (Bundesgerichtshof, 2018).

V. Conclusiones

En primer lugar se debe señalar que, sin lugar a duda, las personas con perfiles digitales pueden establecer, por medio del testamento, su voluntad en el plano digital, pudiendo designar a alguna persona vinculada a ellos o

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

algún heredero, para que éste se dirija a los prestadores de servicios de la información y proceda a la ejecución de su última voluntad en este campo. Situación que, incluso, se puede llevar a través de las personas autorizadas, a tal efecto, por menores o por personas incapaces.

Con este tipo de disposiciones de última voluntad, los usuarios de los servicios de la sociedad de la información podrían ordenar el cierre de sus perfiles o bien la conservación de los mismos, aunque la mayoría de los prestadores de servicios ya cuentan con este tipo de remedios para mitigar su falta de regulación en una norma jurídica.

Aunque es loable la intencionalidad de la nueva Ley de Voluntades Digitales de Cataluña, resulta insuficiente, pues resuelve de manera parcial y escasa la problemática. Básicamente, traslada a una norma los remedios que los prestadores de servicios tienen implementados, sin prever cuestiones prácticas como las contenidas en la Ley francesa para una república digital.

Aunque ya se prevean en la LOPDGDD las facultades de determinadas personas, autorizadas para acceder, oponerse o suprimir los datos de las personas fallecidas, además de lo relativo a lo que la ley denomina "testamento digital". Es urgente desarrollar una reglamentación específica, que señale cómo se debe informar a los servicios de la sociedad de la información sobre la decisión del fallecido respecto a su huella digital, y apostar por una verdadera autodeterminación con efectos *post mortem*, lo cual implica la facultad de decisión de las personas sobre la eliminación o conservación de sus perfiles digitales a su muerte; así como el cumplimiento eficaz de los proveedores de servicios de este tipo de disposiciones, pues la permanencia en línea de los perfiles de la personalidad de su titular (fallecido), son un blanco potencial a intromisiones al derecho al honor, a la propia imagen y a la intimidad personal y familiar. Sin olvidar el hecho de seguir siendo parte de las estadísticas comerciales de las multinacionales.

Observando las políticas de uso de *Google* —en lo referente a la posibilidad de descargar el contenido de una cuenta inactiva, por causa de muerte, a usuarios autorizados por el fallecido para tal efecto— y a lo establecido en la LOPDGDD, considero que se puede generar una colisión de derechos, por la situación que enfrentan las personas autorizadas para acceder al contenido digital de la persona fallecida, frente a los derechos personalísimos de las personas vivas, como sería el secreto a las comunicaciones y el derecho a la protección de datos personales.

Los contenidos de los perfiles digitales tampoco están exentos de verse afectados por la muerte de su titular. Esta situación abre un abanico de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

posibilidades prácticas inimaginables que, sin duda, merecen un estudio específico.

VI. Medios utilizados

Alonso Pérez, Mariano, 2003, "Daños causados a la memoria del difunto y su reparación", Salamanca, recuperado el 26 de noviembre de 2019, disponible en *http://www.asociacionabogadosrcs.org/congreso/ponencias3/PonenciaMarianoAlonsoPerez.html*.

Bodas Daga, Ma. Eugenia, 2007, *La defensa post mortem de los derechos de la personalidad*, Barcelona, Bosch.

Boto Álvarez, Alejandra, 2017, "Transformaciones estructurales en la administración francesa: Cuestiones éticas y tecnológicas", *Revista General de Derecho Administrativo*, núm. 44, recuperado el 26 de noviembre de 2019, disponible en *http://laadministracionaldia.inap.es/noticia.asp?id=1507243*.

Bundesgerichtshof, III ZR 183/17, 2018, disponible en *http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2018-7-12&nr=86602&pos=2&anz=8)*.

Burke, Maureen, 2017, "Un futuro incierto", *Finanzas y desarrollo*, F. M. Internacional, núm. 5, recuperado el 11 de noviembre de 2019, disponible en *https://www.imf.org/external/pubs/ft/fandd/spa/2017/06/pdf/fd0617s.pdf*.

Carta de Derechos Fundamentales de la Unión Europea (CDFUE), 2000, recuperado el 12 de noviembre de 2019, disponible en *http://www.europarl.europa.eu/charter/pdf/text_es.pdf*.

Código Civil, 1889, Real Decreto del 24 de julio de 1889 por el que se Publica el Código Civil, 4 de agosto de 2018, recuperado el 11 de noviembre de 2019, disponible en *https://www.boe.es/buscar/act.php?id=BOE-A-1889-4763&tn=6&p=20180804*.

Constitución Española (CE), 1978.

Directiva 2015/1535 del Parlamento Europeo y del Consejo por la que se Establece un Procedimiento de Información en Materia de Reglamentaciones Técnicas y de Reglas a los Servicios de la Sociedad de la Información, 9 de septiembre de 2015.

Écija Bernal, Álvaro, 2017, "Ciberespacio, ciberderecho, ciberabogados", *Diario La Ley*, núm. 8944.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Facebook, 2019, "Solicitud especial para la cuenta de una persona fallecida o incapacitada", recuperado el 11 de noviembre de 2019, disponible en *https://www.facebook.com/help/contact/228813257197480*.

González Granado, Javier, 2016, "Sólo se muere una vez: ¿Herencia digital?", en Oliva León, Ricardo y Valero Barceló, Sonsoles (coords.), *Testamento ¿digital?*, Juristas con Futuro, recuperado el 11 de noviembre de 2019, disponible en *http://www.juristasconfuturo.com/desafios-legales/ebook-no-1-testamen*.

Google, 2019, "Solicitud relacionada con la cuenta de un usuario fallecido", recuperado el 11 de noviembre de 2019, disponible en *https://support.google.com/accounts/troubleshooter/6357590?hl=es#ts=6357586*.

Google, "Administrador de cuentas inactivas", disponible en *https://myaccount.google.com/inactive*.

Grupo de Trabajo del Artículo 29 (GT 29), 2009, Dictamen 5/2009 sobre las Redes Sociales en Línea.

Hootsuite, 2019, *Global Report. Digital 2019*, recuperado el 11 de noviembre de 2019, disponible en *https://hootsuite.com/pages/digital-in-2019#accordion-115547*.

Instagram, 2019, "Solicitud de cuenta conmemorativa de una persona fallecida en *Instagram*", recuperado el 11 de noviembre de 2019, disponible en *https://help.instagram.com/contact/452224988254813?helpref=faq_content*.

Instagram, 2012, "Comunicado *blog* oficial de *Instagram*", recuperado el 11 de noviembre de 2019, disponible en *http://blog.instagram.com/post/20785013897/instagram-facebook*.

Kammergericht, 2017, *Digitales Erbe im Internet: Anspruch der Eltern auf Gewährung von Zugriff auf den Social-Media-Account ihres verstorbenen minderjährigen Kindes*, 31 de mayo de 2017, disponible en *http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/portal/t/19iy/bs/10/page/sammlung.psml?doc.hl=1&doc.id=KORE242682017&documentnumber=7&numberofresults=14&doctyp=juris-r&showdoccase=1&doc.part=L&paramfromHL=true#focuspoint*.

Lacruz Berdejo, José Luis, 2008, *Elementos de derecho civil III*, 3a. ed., Madrid, Dykinson.

León Robayo, Edgar Iván, 2006, "La posesión de los bienes inmateriales", *Revista de Derecho Privado*, núm. 36, disponible en *https://www.redalyc.org/pdf/3600/360033184002.pdf*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Ley 10/2017 de las Voluntades Digitales y de Modificación de los Libros Segundo y Cuarto del Código Civil de Cataluña, 27 de junio de 2017, disponible en *https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-8525*.

Ley 10/2008 del Libro Cuarto del Código Civil de Cataluña, relativo a las Sucesiones, 10 de julio de 2008, disponible en *https://www.boe.es/buscar/act.php?id=BOE-A-2008-13533*.

Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), 11 de julio 2002, apartado c) del anexo.

Ley Fundamental de la República Federal de Alemania, recuperado el 12 de noviembre de 2019, disponible en *https://www.btg-bestellservice.de/pdf/80206000.pdf*.

Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, 5 de diciembre de 2018, recuperado el 12 de noviembre de 2019, disponible en *https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf*.

Ley Orgánica (LO) 1/1982, del 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, artículos 2.2, 4.3, 6 y 9.6.

LinkedIn, "Formulario para la eliminación de la cuenta de un usuario fallecido", recuperado el 12 de noviembre de 2019, disponible en *https://www.linkedin.com/help/linkedin/ask/ts-rdmlp*.

Llopis Benlloch, José C., 2016, "Con la muerte digital no se juega: el testamento *online* no existe", en Oliva León, Ricardo y Valero Barceló, Sonsoles (coords.), *Testamento ¿digital?*, Juristas con Futuro, recuperado el 11 de noviembre de 2019, disponible en *http://www.juristasconfuturo.com/desafios-legales/ebook-no-1-testamen*.

Loi no. 2016-1321 du 7 de Octobre pour une République Numérique, artículo 63.2, 2016, recuperado el 12 de noviembre de 2019, disponible en *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id#JORFARTI000033203260*.

Pascual Medrano, Amelia, 2003, *El derecho fundamental a la propia imagen. Fundamento, contenido y límites*, Navarra, Aranzadi.

Piñar Mañas, José Luis, 2019, "¿Qué regulación de los derechos en la sociedad digital?", *Derecho Digital e Innovación*, núm. 1, enero-marzo, el 11 de noviembre de 2019.

Piñar Mañas, José Luis, 2018, "Identidad y persona en la sociedad digital", en Piñar Mañas, José Luis, *Sociedad digital y derecho*, Madrid, Boletín Oficial del Estado, recuperado el 11 de noviembre de 2019, disponible

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

en *https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-NT-2018-97*.

Project de Loi pour une République Numérique, 2015, Exposición de motivos del proyecto de la ley para una república digital, recuperado el 12 de noviembre de 2019, disponible en *http://www.assemblee-nationale.fr/14/projets/pl3318.asp*.

Real Decreto Legislativo 1/1996 por el que se Aprueba el Texto Refundido de la Ley de Propiedad Intelectual, Regularizando, Aclarando y Armonizando las Disposiciones Legales Vigentes sobre la Materia, 12 de abril de 1996.

Reglamento de la Organización y Régimen del Notariado, artículo 226 a), 2 de junio de 1944, disponible en *https://www.boe.es/buscar/act.php?id=BOE-A-1944-6578*.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 27 de abril de 2016 (o Reglamento General de Protección de Datos), recuperado el 12 de noviembre de 2019, disponible en *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679*.

STC 7/2019, 17 de enero de 2019 (Pleno), Recurso de Inconstitucionalidad 4751-2017. Interpuesto por el Presidente del Gobierno en Relación con Diversos Preceptos de la Ley del Parlamento de Cataluña 10/2017, del 27 de junio, de las Voluntades Digitales y de Modificación de los Libros Segundo y Cuarto del Código Civil de Cataluña. Competencias sobre ordenación de los registros públicos de derecho privado: nulidad de los preceptos legales autonómicos relativos a la ordenación de voluntades digitales en ausencia de disposiciones de última voluntad, designación de persona encargada de ejecutar las últimas voluntades, registro electrónico de voluntades digitales y mediación para resolver las discrepancias surgidas en aplicación de la ley. Voto particular, ECLI:ES:TC:2019:7, recuperado el 12 de noviembre de 2019, disponible en *https://www.boe.es/boe/dias/2019/02/14/pdfs/BOE-A-2019-2033.pdf*.

STC 103/1999, 3 de junio de 1999 (Pleno), ECLI: ES:TC:1999:103, recuperado el 12 de noviembre de 2019, disponible en *http://hj.tribunalconstitucional.es/es/Resolucion/Show/3845*.

STC 87/1985, 16 de julio de 1985, ECLI:ES:TC:1985:87, disponible en *http://hj.tribunalconstitucional.es/es/Resolucion/Show/467*.

STC 32/1983, 28 de abril de 1983, ECLI:ES:TC:1983:32, disponible en *http://hj.tribunalconstitucional.es/es/Resolucion/Show/160*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Twitter, "Formulario de privacidad", recuperado el 11 de noviembre de 2019, disponible en *https://support.twitter.com/forms/privacy*.

Yahoo!, "Página de ayuda de *Yahoo!*", recuperado el 11 de noviembre de 2019, disponible en *https://es-us.ayuda.yahoo.com/kb/SLN26544.html*.

Zuckerberg, Mark, 2019, Publicación de *Facebook* del 10 de abril, disponible en *https://www.facebook.com/zuck*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES EN LA CADENA DE BLOQUES (*BLOCKCHAIN*)

TRANSPARENCY AND PROTECTION OF PERSONAL DATA IN THE BLOCKCHAIN

Jersain Zadamig LLAMAS COVARRUBIAS*

RESUMEN. Cada día son más las amenazas en torno al tema de la violación de datos personales, donde la privacidad y seguridad de la información son el principal reto en esta era de la información y comunicación. La tecnología *Blockchain* llega como una revolución por sus características de inmutabilidad, confianza, transparencia, descentralización y distribución en los registros, convirtiéndola en una tecnología disruptiva que llega a romper los paradigmas tradicionales respecto a cómo percibimos el mundo. En su desarrollo y aplicación, nos plantea muchas interrogantes, principalmente con la compatibilidad, privacidad y protección de datos personales, razón por la cual se examinará de manera general cómo funciona esta tecnología disruptiva, la intersección que tiene con las normas legales, y las posibles encrucijadas en que deberán dialogar y resolverse, para que las personas sean verdaderos dueños de su identidad y de sus datos personales.

PALABRAS CLAVES. *Blockchain*, protección de datos personales, transparencia, transmisión de datos.

* Abogado y maestro en Derecho constitucional y administrativo por la Universidad de Guadalajara. Especializado en Derecho y nuevas tecnologías de la información y comunicación. Cofundador de Legal Hackers Guadalajara. *jersain@protonmail.com.*

Fecha de recepción: 21 de julio de 2019.
Fecha de dictamen: 11 de septiembre de 2019.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

ABSTRACT. Every day there are more threats in the violation of personal data, where privacy and security of information are the main challenge in this age of information and communication. Thus, Blockchain technology comes as a revolution due to its characteristics of immutability, trust, transparency, decentralization and distribution in the registers, turning it into a disruptive technology that breaks traditional paradigms about how we perceive the world. In its development and application, it raises many questions, mainly with the compatibility, with privacy and protection of personal data, which is why we will examine in a general way how this disruptive technology works, the intersection it has with the legal norms and the possible crossroads they must dialogue and resolve so that people are true owners of their identity and personal data.

KEYWORDS. Blockchain, protection of personal data, transparency, data transmission.

I. Introducción

La idea de que ningún derecho puede ser absoluto, en razón de que existen otros derechos que también deben ser protegidos, y por lo tanto, los derechos de acceso a la información y protección de datos personales pueden ser limitados de manera excepcional, es válida en el sentido de que ningún poder constituyente ni constituido puede prever todos los posibles casos y consecuencias.

Por otra parte, existe una teoría de clasificación de derechos: primero, los derechos universales absolutos, como el derecho a la vida y la libertad; segundo, los derechos universales relativos, como los derechos sociales y a la salud, educación o similares; tercero, los derechos singulares absolutos, como la propiedad privada y los demás derechos reales; y por último, los derechos singulares relativos, como los derechos de crédito y otros derechos personales (Ferrajoli, 2011: 621). Es así como podemos entender la progresividad de los derechos y su cumplimiento por los Estados.

Lo anterior no exime que los derechos de transparencia, acceso a la información y protección de datos personales sean incumplidos, al no ser derechos universales absolutos, además de estar a la dispensa de la legislación de los Estados, pues ésta debe cumplirse en la mayor medida posible.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Prima facie, con la tecnología *Blockchain*, podríamos creer que se garantizan derechos básicos regulados en la legislación internacional y nacional; sin embargo, existe un catálogo más amplio de derechos originarios y otros derivados que pueden garantizarse. Tal es el caso del derecho de protección de datos personales con los derechos ARCO (acceso, rectificación, cancelación y oposición), *habeas data* y derecho al olvido; así mismo se contempla el derecho a la intimidad, derecho a la privacidad, derecho al anonimato, derecho a encriptar, derecho al honor, derecho a la libertad de expresión, derecho de transparencia, acceso a la información pública y rendición de cuentas, derecho a la verdad, derecho a la no censura, derecho al uso de *software* libre, derecho a la auditoría o auditabilidad del código fuente y derecho a la gobernanza electrónica (Llamas y Llamas, 2018: 88-162).

Nos encontramos en una intersección fundamental entre el derecho y la tecnología, que incluso podría compararse con el auge del internet, pues es posible que todos los paradigmas evolucionen y tengamos una nueva percepción del mundo, introduciendo verdaderos principios de autodeterminación informativa, de privacidad y transparencia inmutable ante la sociedad, razón por la cual en los siguientes capítulos se intentará explicar cómo funciona la tecnología *Blockchain*, con sus conceptos básicos y conocimientos técnicos a un nivel general, aunado a comentar las encrucijadas y posibles colisiones con las legislaciones actuales: tanto la nacional, en el caso de México, como la internacional, con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

II. *Blockchain*

1. *Concepto*

La tecnología *Blockchain* nació gracias a la persona o entidad anónima llamada Satoshi Nakamoto, la cual publicó en 2008 un artículo titulado "Bitcoin: A Peer-to-Peer Electronic Cash System" (en español: "*Bitcoin*: un Sistema de Efectivo Electrónico Usuario-a-Usuario"). En 2009, presentó el *software* de *Bitcoin*, creó la red y propuso la criptomoneda *bitcoin*. Cabe aclarar que en el mundo de las criptotecnologías, se hace referencia a *Bitcoin* (con "B" mayúscula) como la red, y a *bitcoin* (con "b" minúscula) como el activo virtual (Filippi y Wright, 2018: 3).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Blockchain es un conjunto de tecnologías que se comporta como un sistema descentralizado y distribuido, mecanismo de consenso, con redes de persona a persona y sistemas criptográficos. *Blockchain* ha llegado a innovar, en múltiples sectores, como un medio de acoplamiento o vinculación, pues emerge como un puente entre unidades independientes, donde "ante distintas variables adoptan los mismos valores o valores complementarios y que en determinadas ocasiones actúan como un sistema homogéneo" (Luhmann, 1998: 209), creando un sistema que da certeza ante todos los sistemas en sociedad.

Dicho lo anterior, es importante definir qué es *Blockchain*, a la cual también se conoce como la cadena de bloques. Esta tecnología consiste en marcadores digitales, a prueba de manipulaciones y resistentes a las mismas, implementados de manera distribuida (sin un depósito central), y generalmente sin una autoridad central (un banco, empresa o gobierno). Dentro de su nivel básico, permiten a una comunidad de usuarios registrar transacciones en un libro mayor, que es compartido dentro de esa comunidad, de tal modo que, en el funcionamiento normal de la red de *Blockchain*, no se puede cambiar ninguna transacción una vez que ha sido publicada (Yaga *et al*., 2018: 4).

De una manera más clara, *Blockchain* es una tecnología que permite crear redes entre personas, utilizando sus propios dispositivos, sin necesidad de una entidad central, es así que, por su característica de descentralización y distribución, los dispositivos realizan un mecanismo de consenso para llegar a validar transacciones. Esto es gracias a un *software* que, una vez instalado en un dispositivo, descarga toda la cadena de bloques y replica todo el registro en la red, garantizando la inmutabilidad de la misma. Se le puede llamar registro contable o base de datos descentralizada, pero entre sus funciones primigenias se encuentra el ser totalmente transparente, porque se pueden leer los registros por quien desee hacerlo, y a su vez se pueden escribir registros por medio de una transacción que conlleva un proceso de consenso, mediante algoritmos matemáticos y criptográficos.

2. *Funcionamiento general*

No es sencillo explicar la tecnología *Blockchain*. No obstante, a *grosso modo* expresaré su funcionamiento de manera llana y con gráficos. Estos últimos los realicé con base en las ideas del *paper* de Satoshi Nakamoto (2008), donde explica el funcionamiento de *Bitcoin*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Un concepto práctico, para entender a grandes rasgos esta tecnología disruptiva, es:

> Registro compartido de manera distribuida y descentralizada entre múltiples dispositivos, donde las transacciones se registran y validan mediante un mecanismo de consenso, las cuáles son agregadas en bloques unidos con una cadena criptográfica, con el fin de crear marcadores digitales a prueba de manipulaciones y resistentes a la misma. (Quirós, 2019)

Primero, visualicemos que tenemos un registro contable único y universal donde se escriben todas las transacciones, o mejor dicho todos los movimientos válidos que suceden.

Gráfico 1. Registro contable único

Fuente: gráfico hecho con iconos realizados por Freepik en *www.flaticon.com* (Nota: los gráficos obtenidos de *www.flaticon.com*, están bajo una licencia *Creative Commons BY 3.0. http://creativecommons.org/licenses/by/3.0/*).

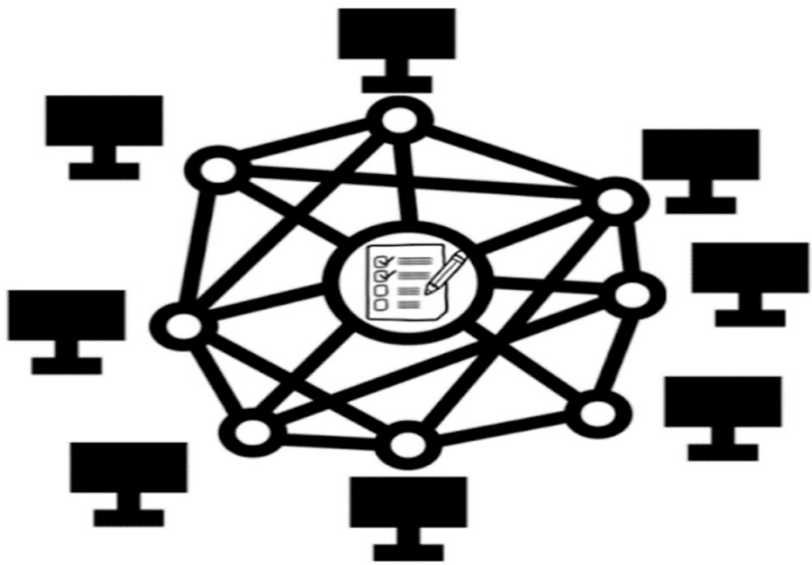
Como segundo punto, dicho registro contable único y universal no se encuentra de manera aislada o centralizada en una única entidad, se encuentra como un registro compartido de manera distribuida y descentralizada entre múltiples dispositivos, es decir, existe una copia en cada dispositivo de la red.

Entonces, la red *Blockchain* es un registro compartido de manera distribuida y descentralizada entre múltiples dispositivos; esto quiere decir que tal registro, base de datos o contabilidad, corre de manera conjunta entre múltiples dispositivos (distribución) en una red, y todos tienen la

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

misma jerarquía (descentralización). Con las tecnologías actuales, estamos acostumbrados a utilizar sistemas centralizados que pueden ser susceptibles de modificación al ser una copia única o una entidad jerárquica única; sin embargo, con *Blockchain* el registro se comparte en todos los dispositivos.

Gráfico 2. Registro compartido, distribuido y descentralizado en múltiples dispositivos



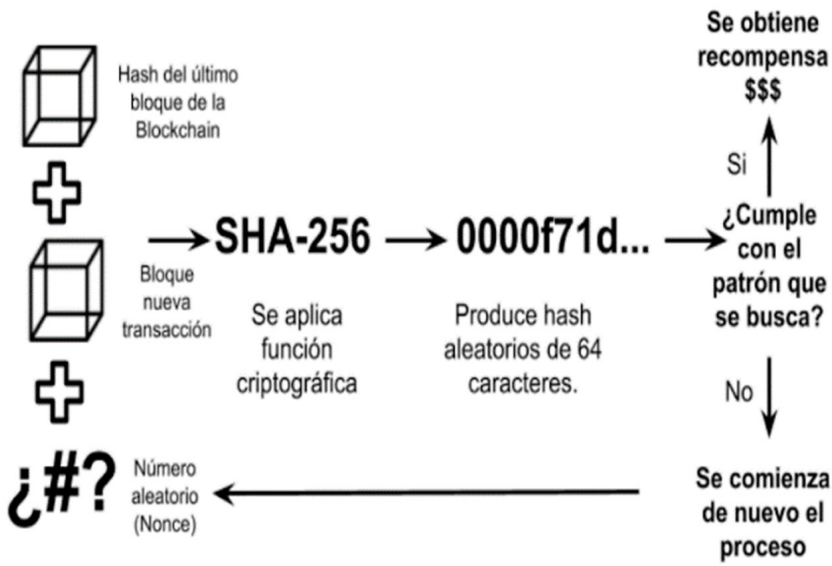
Fuente: gráfico hecho con iconos realizados por monkik & srip en *www.flaticon.com*.

Y aquí nace la siguiente interrogante: ¿cómo se actualizan o sincronizan las copias de la red *Blockchain*? La respuesta, como tercer punto, es que las transacciones se registran y validan mediante un mecanismo de consenso. El consenso es un concepto que atañe a diversas materias, pero en lo que se refiere a *Blockchain*, es un mecanismo para aceptar la verdad individual de todos los miembros dentro de la red. Existen diversos protocolos de consensos: por ejemplo, el "Proof of Work, Proof of Stake, Delegate Proof of Stake, Proof of Elapsed Time, Deposit-based consensus, Proof of Importance, Federated consensus or federated Byzantine consensus, Reputation-based mechanisms, Practical Byzantine Fault Tolerance" (Bashir, 2017: 28-30).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Respecto al mecanismo de consenso, el propuesto por Nakamoto, en su *paper* de *Bitcoin*, es el *Proof of Work* (PoW), o mejor conocido como prueba de trabajo; dicho PoW es un mecanismo en cuya prueba se gastan suficientes recursos computacionales, antes de proponer un valor de aceptación por parte de toda la red. El mismo Nakamoto lo plasmó en su *paper* así: "Una vez que el esfuerzo de CPU se ha gastado para satisfacer la prueba de trabajo, el bloque no puede ser cambiado sin rehacer todo el trabajo" (2008: 3).

Gráfico 3. Protocolo de Consenso *Proof of Work*



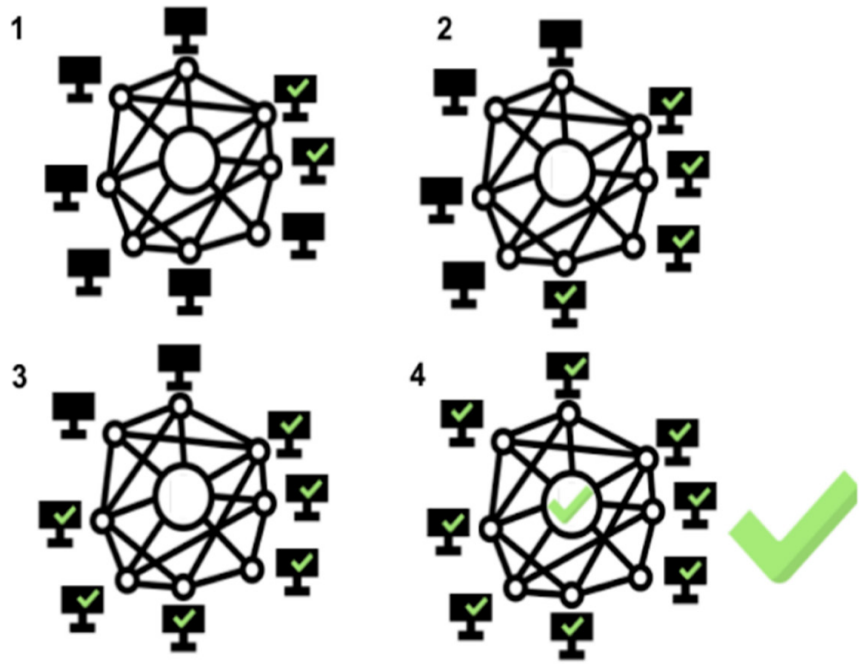
Fuente: gráfico hecho con iconos realizados por Retinaicons en *www.flaticon.com*.

En pocas palabras, un protocolo de consenso es la forma en la que se pondrán de acuerdo los mineros para poder llegar a un acuerdo de mayoría (prueba de trabajo), y poder sincronizar la red *Blockchain* (registro). Cabe destacar que cada bloque es generado aproximadamente cada 10 minutos, y en esto consiste la dificultad del problema. Los mineros tienen que seguir cambiando el *nonce* hasta que se genere el número deseado, como si fuera una lotería produciendo los *hash* de salida en el cifrado *SHA-256*; o también, es como si fuera una carrera en donde tienen ventaja los que poseen los requerimientos de *hardware* con más potencia para generar más

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

hash por segundo. Una vez que se encuentra el *nonce* con el *hash*, éste es transmitido a los otros mineros para verificarlo, aceptarlo y validarlo, y así sucesivamente trabajan en el siguiente bloque.

Gráfico 4. Validación y sincronización del registro único contable de la red *Blockchain* por medio de un protocolo de consenso



Fuente: gráfico hecho con iconos realizados por monkik & Freepik en *www.flaticon.com*.

Y la siguiente duda sería: ya validados, ¿cómo se agregan dichos bloques a la red? La respuesta, como cuarto punto, es que son agregados en bloques unidos con una cadena criptográfica, ofreciendo inmutabilidad, ya que todos los bloques están unidos desde el primer bloque de la red (bloque génesis) hasta el último.

Es necesario puntualizar que cada bloque tiene la huella del bloque anterior, por lo que la cadena es continua, y sólo se permitirán los bloques fidedignos. Respecto a la red de *Blockchain* con marcas de tiempo, que da la inmutabilidad y certeza de la información, funciona al tomar un *hash* de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

un bloque de elementos para ser fechados y publicados. Es decir, la marca de tiempo sirve para reforzar el argumento de que la cadena debió haber existido en el tiempo para adentrarse en el *hash*; es así que, conforme pasen los bloques, más certeza existirá en la información.

Gráfico 5. Transacciones agregadas en bloques unidos con una cadena criptográfica

FUENTE: gráfico hecho con iconos realizados por Freepik en *www.flaticon.com*.

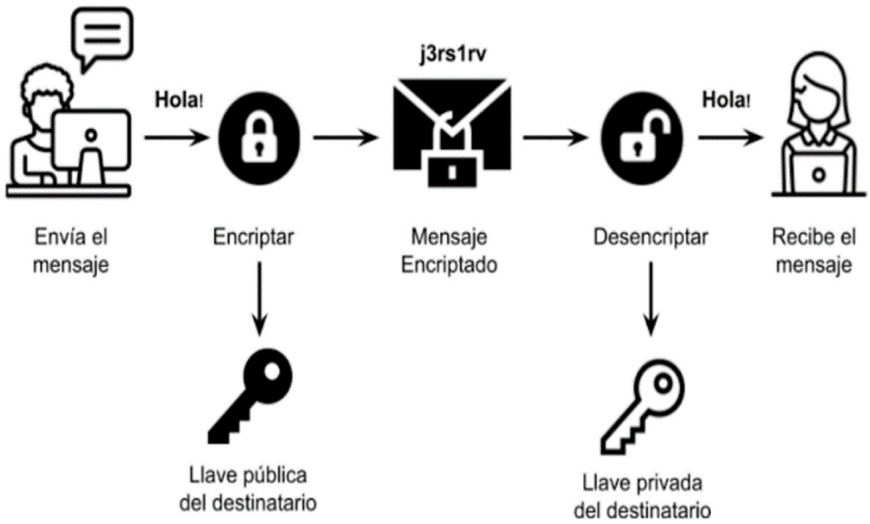
El sistema de cifrado es también muy importante, *Blockchain* utiliza el sistema de llave pública o sistema asimétrico de cifrado, donde podemos entender que se utilizan dos llaves, una pública y otra privada. Por lo tanto, si alguien quiere compartir algo con otra persona, se debe cifrar utilizando la clave pública. Ya cifrada la información, se podrá descifrar obteniendo la clave privada, la cual no debe ser compartida con nadie. Un ejemplo muy sencillo es el de una persona que tiene una casa, donde si quiere utilizar su televisor, su baño, su carro, o cualquier otro objeto que esté dentro de su propiedad, necesitará una llave para entrar a ésta, y así poder hacer uso de todo lo que está dentro. Entonces tal llave le otorga la posesión sobre todo lo que se encuentre ahí; de igual manera, si quisiera solicitar que le enviaran algún artículo comprado, puede especificar que se lo entreguen en su casa, por lo que tendrá que proveer su dirección, la cual identifica su hogar del resto existente. Por lo tanto, una vez que el artículo llega, y la

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

persona recibe el objeto solicitado, éste pasa a ser de su pertenencia: por consecuencia, solamente él puede hacer uso de éste cuando lo desee.

En síntesis, gracias al cifrado de llave o clave pública, cada usuario en la red *Blockchain* posee una llave privada, la cual es única e irrepetible, y es capaz de descifrar la información ligada a su llave pública. Es así que, si bien la información puede ser procesada o vista por todos los participantes de una red, el único dueño de dicha información, capaz de decidir sobre la misma, es su titular con su llave privada.

Gráfico 6. Cifrado asimétrico (llave pública)



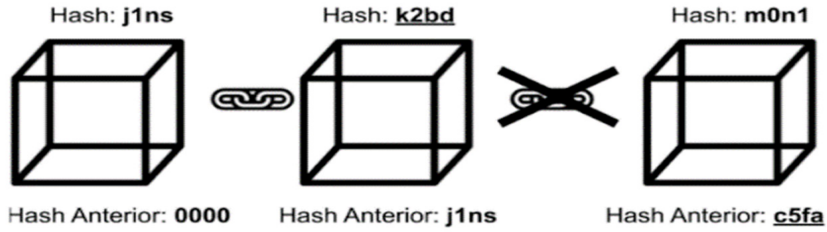
Fuente: gráfico hecho con iconos realizados por Freepik & Chanut en *www.flaticon.com*. Basado en McAndrew (2011: 4).

Por consiguiente, ¿qué pasaría si alguien quiere modificar la red o por qué *Blockchain* es inmutable? La respuesta, como quinto punto, es que al estar todos los bloques conectados (en cadenas continuas), se crean marcadores digitales a prueba de manipulaciones y resistentes a la misma.

En una entidad centralizada, la manipulación de la información es sencilla, pero en un sistema descentralizado es teóricamente imposible alterarla. Dicho sistema es inmutable, pues en el momento en que se intente enviar una transacción inválida o con información apócrifa, éstos son detectados y eliminados de la red, preservando la confiabilidad del sistema.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Gráfico 7. Bloques con marcadores digitales a prueba de manipulaciones y resistentes a la misma



Fuente: gráfico hecho con iconos realizados por Freepik & Retinaicons en *www.flaticon.com*.

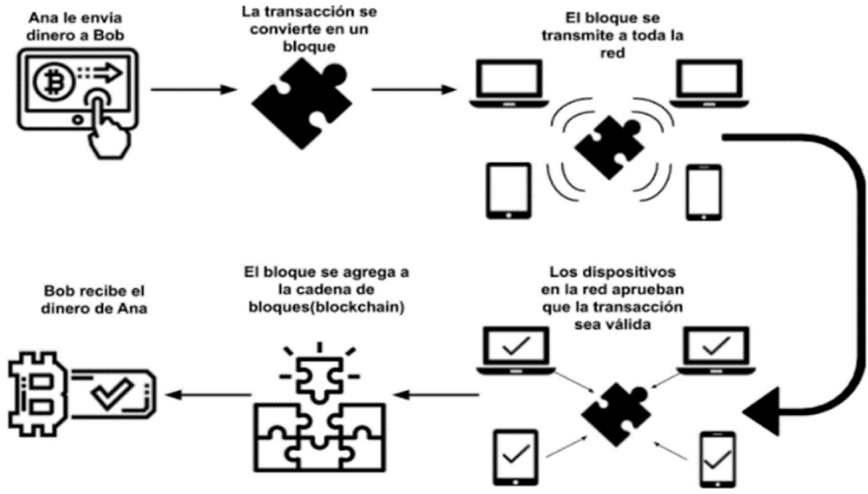
Por último, y como sexto punto: ¿cómo se mantiene la red? La respuesta es que se participa activamente en la red, creando nuevos bloques constantemente y de manera sincronizada; se hace resolviendo un problema difícil, y por esto se llama prueba de trabajo. Así que cuando se resuelve el problema (*nonce*), el minero recibe un incentivo o recompensa; esto es importante, ya que el incentivo hace que la propia red se mantenga; a esto podríamos denominarlo como un sistema autopoiético, donde se reproduce y se mantiene por sí mismo, pues "un sistema que dispone de estructuras y procesos propios puede coordinar con estas formas del fortalecimiento de selección todos los elementos que produce y reproduce; puede así regular su propia autopoiesis" (Luhmann, 1998: 65).

Es así que *Blockchain* ofrece transparencia al poder ligar todas las transacciones —inclusive desde el principio hasta el final de la cadena— al estar conectadas en bloques unidos, lo que a su vez ofrece inmutabilidad por sus marcadores digitales. A continuación se ejemplifica, y se expresa de manera gráfica, un funcionamiento global de *Blockchain*.

Ejemplo: Si Ana le quiere enviar dinero a Bob, puede realizar diversos métodos de pago, pero todos con entidades centralizadas y con un *fee* (impuesto) altísimo de transacción. Pero si utiliza *Blockchain*, todos los usuarios que estén en la red pueden validar la transacción de una forma más económica, rápida, segura e inmutable. De una manera breve: cuando Ana le envía dinero a Bob mediante esta red, la transacción se convierte en un bloque que se transmite a toda la red, y en dicha red los dispositivos aprueban que la transacción es válida, por medio de un mecanismo de consenso. Tras la validación, el bloque se agrega a la cadena de bloques (*Blockchain*) y Bob recibe su dinero.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Gráfico 8. Funcionamiento general de una transacción en *Blockchain*



FUENTE: gráfico hecho con iconos realizados por Freepik, surang & geotatah en *www.flaticon.com*.

III. TRANSPARENCIA Y *BLOCKCHAIN*

Blockchain impulsa nuevas formas de organización más transparentes y descentralizadas, y gracias a la naturaleza transparente y abierta de estas redes, la cadena de bloques funciona en múltiples ordenadores y dispositivos.

Blockchain permite un sistema resistente al cambio, posibilitando un almacenamiento de datos con no repudio, es decir que no se pueda negar que la información se realizó por el autor originario de cada movimiento, de manera no anónima, pero sí pseudoanónima y transparente, donde todas las transacciones pueden verificarse; incluso, dicha tecnología es tan transparente y trazable, que abre la puerta a la rendición de cuentas, por ser un vehículo de vigilancia y control.

La información mantenida en una cadena de bloques se autentica, y los metadatos y otra información contextual sobre las transacciones basadas en cadenas de bloques están disponibles para que otros puedan verlas. Cualquiera puede descargar una cadena de bloques y evaluar si una cuenta determinada estuvo involucrada en una transacción (Filippi y Wright, 2018: 37).

Es muy importante puntualizar, como ya se mencionó anteriormente, que la cadena de bloques está almacenada en un registro de manera

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

secuencial, con marca de tiempo por partes, debidamente autenticadas, y que dicho registro es accesible y auditable por cualquier persona con conexión a internet. Permitiendo así que existan registros, no únicamente financieros, sino de todo tipo, con la cualidad de ser transparentes, a prueba de manipulaciones y con un sello de tiempo de cada operación (movimiento).

La tecnología puede servir como una columna vertebral para los registros gubernamentales, proporcionando a los ciudadanos acceso a la información a pedido, y utilizando el dispositivo de su elección (Filippi y Wright, 2018: 109).

Desde un punto de vista técnico, la cadena de bloques es una base de datos distribuida, transparente, inmutable, validada, segura y pseudoanónima que existe como nodos múltiples, de modo que si el 51% de los nodos honestos está de acuerdo, la confianza de la cadena está garantizada (Bambara y Allen, 2018: 6).

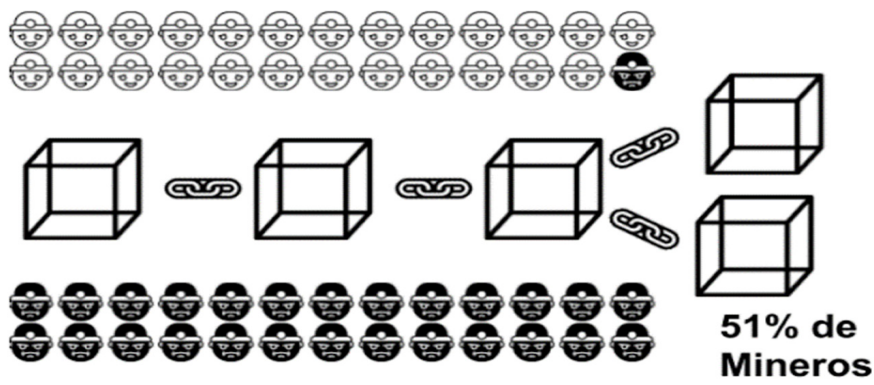
No obstante, con la característica de inmutabilidad que otorga la *Blockchain*, se llega a una certeza en la transparencia y rendición de cuentas. Sin embargo, antes de hablar de transparencia de los datos procesados en la red, primero debe existir una transparencia en el código fuente computacional de la red *Blockchain*, con el fin de conocer las funcionalidades de la red y no caer en el supuesto de promover un sistema descentralizado y distribuido, pero que materialmente sea un sistema centralizado.

Como segundo punto, la inmutabilidad de la información es puesta en duda, principalmente en las redes *Blockchain* privadas, o mejor dicho en las *Distributed Ledger Technology* (DLT), y pese a los diferentes tipos de protocolos de consenso que se mencionaron anteriormente, el más conocido y usado es la prueba de trabajo o *Proof of Work*, en virtud de que debe existir un consenso mayoritario al 51% de los participantes de la red, para poder sincronizar la información.

En un argumento contrario, puede existir un ataque del 51% en donde se pueda manipular un registro en la red *Blockchain*, en caso de que un grupo de atacantes se involucre y cumpla con una mayoría de participantes para hacerse cargo de la red de modo efectivo, y apruebe transacciones a un ritmo que supere al resto, es decir al 49% (Filippi y Wright, 2018: 25). Actualmente, este supuesto es meramente teórico, ya que no ha ocurrido un ataque de esta manera, principalmente porque es difícil y costoso llevarlo a cabo, pero las redes privadas o DLT podrían efectuarlo por estar permisionadas y ser de un grupo o consorcio de participantes que pudieran acordarlo. Enseguida, en el gráfico 9, se muestra un ejemplo de ataque del 51% en una red.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

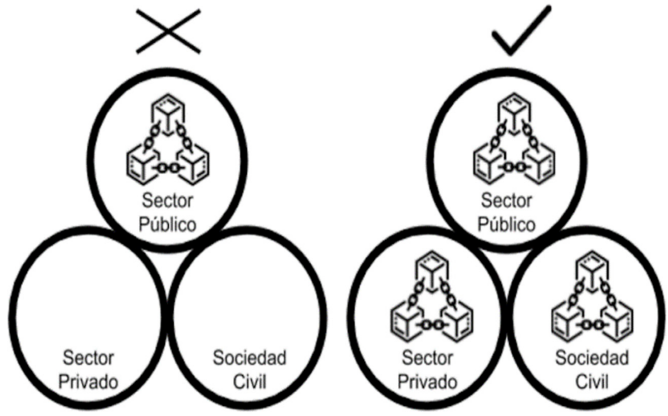
Gráfico 9. Ataque del 51%



FUENTE: gráfico hecho con iconos realizados por Freepik, Retinaicons & Creaticca Creative Agency en *www.flaticon.com*.

En el mismo orden de ideas, también debe surgir una red *Blockchain* en sinergia con una gobernanza entre el sector público, sector privado y sociedad civil organizada, donde ninguna entidad o grupos mayoritarios (51% de participantes en la red) tengan la posibilidad de manipular los registros, atacando la transparencia de la información y rendición de cuentas en las sociedades democráticas.

Gráfico 10. Gobernanza y cadena de bloques



FUENTE: gráfico hecho con iconos realizados por Freepik en *www.flaticon.com*.

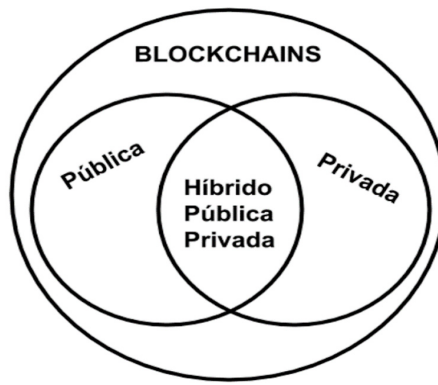
DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Otro problema que podemos encontrar en la transparencia de *Blockchain* es la estricta transparencia *per se*, pues aunque es una característica primordial de esta tecnología, en algunos casos no sería tan viable por su inexacta implementación. Si bien en este mundo existen reglas y principios —"los principios son mandatos de optimización y las reglas, como normas que sólo pueden ser cumplidas o no" (Alexy, 1993: 98)—, las reglas simplemente pueden cumplirse o no, pero los principios, como elementos abstractos, deben optimizarse para cumplirse de la mejor forma posible.

Dicho lo anterior, al ser *Blockchain* una tecnología incorruptible, inmutable, eficaz y confiable al cumplir todas las reglas, se subsume a lo que se condiciona y acepta, pero aquí es cuando tendremos que preguntarnos si *Blockchain* puede involucrar un nivel de transparencia que proteja los intereses jurídicos de confidencialidad y reserva de la información, pues ¿qué pasa si las partes no quieren que se divulguen los detalles? o ¿cómo se mantienen privados los registros cuando sea necesario?

Por ejemplo, no es viable una transparencia total respecto a información acerca de una cadena de información militar o de salud. En estos casos, se debe limitar quién tiene acceso para leer y escribir en esa *Blockchain*. De acuerdo con un informe publicado por el Centro Internacional de Investigaciones para el Desarrollo de Canadá, existen diferentes tipos de clasificaciones, como la pública, privada o DLT e híbrida (Zambrano, 2017: 29). Donde según lo que se necesite implementar, es el tipo de *Blockchain* que se deberá seleccionar, por lo que es necesario, previo a su implementación, llevar a cabo un análisis exhaustivo sobre qué tipo de red es necesario asentar.

Gráfico 11. Tipos de *Blockchain*



Fuente: gráfico hecho con base en Zambrano, 2017: 29.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Se reitera que se encuentran tres tipos de *Blockchain* (públicas, privadas e híbridas). Primero, las públicas o sin permiso, las cuales no son propiedad de nadie, están abiertas al público y todos pueden participar en el proceso de toma de decisiones; así mismo, la recompensa es fundamental para los participantes, y todos los usuarios mantienen una copia del libro de contabilidad en sus registros, utilizando mecanismos de consensos distribuidos para la toma de decisiones. Por otra parte, la *Blockchain* privada, o con permisos, también conocidas como DLT, "son un consorcio o grupo de individuos u organizaciones que deciden compartir un libro distribuido entre ellos" (Bashir y Prusty, 2019: 31).

En lo que respecta a las redes híbridas, son una combinación entre lo público y lo privado, pues tiene una autorización parcialmente privada, y es usada en grupos de compañías o por un consorcio; un ejemplo de éstas podría ser un sistema que trate datos personales médicos, militares o corporativos, en los cuales se quiera mantener ciertos datos de manera privada y controlada, pero a la vez aprovechar todas las herramientas y certeza que brinda una *Blockchain* pública.

En el caso de las redes privadas, o mejor dicho DLT, la cuestión de inmutabilidad de la información es relativa, ya que "a pesar de que el *Blockchain* es inmutable por su diseño, todavía existen riesgos de seguridad incluso con las redes privadas de *Blockchain* con permiso" (IBM, 2018: 4), esto se debe principalmente al acceso no autorizado; mientras que en las redes públicas, por su propia naturaleza de descentralizado y distribuido, teóricamente es imposible cambiar la información, es decir: su inmutabilidad impera por tener los nodos y copias en todo lugar.

Es fundamental conocer los tipos de redes *Blockchain*, para poder cumplir con la normatividad en materia de transparencia y protección de datos personales.

Si bien, por ahora, la tecnología *Blockchain* sigue creciendo, llegará el momento en que cambiará la forma con la que percibimos el mundo. Tal como lo expresa Melanie Swan (2015), dentro de esta tecnología podremos encontrar diversas generaciones: en donde *Blockchain* 1.0 es la moneda; la 2.0, los contratos inteligentes; y la 3.0, las aplicaciones de justicia, más allá de la moneda, la economía y los mercados. Razón por lo cual habrá que indicar *a priori*, qué registros deben ser transparentes y cuáles no.

IV. Protección de datos personales y *Blockchain*

En el panorama actual, se cuenta con el RGPD, documento expedido por la Unión Europea, cuya aprobación fue en 2016 y su aplicación en 2018.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

En México, contamos con un marco constitucional que garantiza el derecho fundamental de protección de datos personales, sujeto a los artículos 6o. y 16 de nuestra carta magna, de éstos se desprende la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), expedida en 2010, y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), expedida en 2017.

Ambas legislaciones no fueron elaboradas en concordancia con la tecnología *Blockchain*, por lo tanto, tendrán que evolucionar ante los cambios disruptivos. Lo anterior no exime a que sea totalmente incompatible esta tecnología con las normas jurídicas, pues en una interpretación extensiva y evolutiva, se pudiera adaptar la red *Blockchain* en armonía con los ordenamientos jurídicos.

En el caso de México, la LGPDPPSO define el concepto de cómputo en la nube como "modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente" (artículo 3, fracción VI). De la definición anterior, se debe resaltar la palabra distribuido; pero, antes de pensar en una hipótesis, es necesario explicar los servicios de computación en la nube.

Brevemente, en los servicios en la nube encontramos el "*Software-as-a-Service* (SaaS), *Platform-as-a-Service* (PaaS), *Infrastructure-as-a-Service* (IaaS)" (Erl *et al.*, 2015: 478-483); de los cuales: el SaaS es un servicio que el usuario puede utilizar sin la necesidad de instalar o ejecutar un *software* de manera local; por ejemplo, *Google Drive*, específicamente *Google Docs*, con su editor de texto. El PaaS es una plataforma que permite desarrollar aplicaciones y ofrecer servicios sin necesidad de instalar *software*; por ejemplo, *Google App Engine*. El IaaS es un servicio *online* que permite pagar por recursos de *hardware*; por ejemplo, *Amazon Web Services* renta servicios de hospedaje y procesamiento.

Es así que *Blockchain* llega como un servicio en la nube que madura todos los servicios contemporáneos, entonces la definición de cómputo en la nube y la palabra distribuido, en la definición legal de la LGPDPPSO, abre la puerta para permitir la *Blockchain-as-a-service* (BaaS): "con el servicio de cadena de bloques de Azure, Microsoft se convirtió en el primer proveedor de *software* en lanzar en 2015. Microsoft, en estrecha colaboración con *ConsenSys*, anunció desarrollar un *Ethereum* BaaS en la plataforma de Microsoft Azure" (Gupta, 2018: 78).

Por otra parte, existen varios asuntos que deben considerarse, antes de que las personas utilicen la cadena de bloques. Como primer asunto,

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

tenemos la inmutabilidad de la información que provee, por su naturaleza, la cadena de bloques, y como antítesis los derechos de rectificación, cancelación, oposición o el derecho al olvido y/o el de borrado, además la transmisión o transferencia de los datos personales en una red distribuida y descentralizada.

Otra interrogante es saber si los datos procesados por la tecnología *Blockchain* son considerados como datos personales, pues al ser cifrados bajo una función *hash*, pudieran llegar a ser datos seudonimizados o anonimizados (RGPD); en el caso de México, datos disociados (artículo 3, fracción XIII, LGPDPPSO), y por ende no recabar el consentimiento del titular (artículo 22, fracción IX, LGPDPPSO), o como lo marca el considerando 26 del RGPD: "los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo", creando un posible escenario fuera de la regulación de protección de datos, con la justificación de que con esta tecnología nos encontramos ante datos anonimizados al no ser identificables, o en contrario, ante datos seudonimizados que pueden ser identificables, y por ende, bajo la potestad de las regulaciones en protección de datos personales.

En México, un dato personal es cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información (artículo 3, fracción IX, LGPDPPSO). Mientras que, en Europa, es toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (artículo 4, 1), RGPD).

Respecto al tratamiento de los datos, el RGPD deja fuera los datos anónimos, pues como lo dice en el considerando número 26:

> los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuen-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

cia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

Lo anterior concluye que los datos anónimos no son sujetos a la legislación internacional, pero habría que considerar si los datos anónimos son funcionales para las tareas diarias.

Por otra parte, la Agencia Española de Protección de Datos también se manifiesta respecto a los datos anonimizados, diciendo que la finalidad del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados, manteniendo la veracidad de los resultados del tratamiento de los mismos; es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleve una distorsión de los datos reales (2016: 2).

Por otra parte, el Grupo de Trabajo del Artículo 29 aborda el mismo tema de datos de anonimización, comentando que para anonimizar cualesquiera datos es necesario eliminar de ellos los elementos suficientes para que no pueda identificarse al interesado. Con más precisión, hay que tratarlos de tal manera que no puedan usarse para identificar a una persona física mediante "el conjunto de los medios que puedan ser razonablemente utilizados" por el responsable del tratamiento o por terceros. Un factor importante al respecto es que el tratamiento debe ser irreversible (2014: 5-6).

Dicho Grupo de Trabajo del Artículo 29 —órgano consultivo europeo independiente que aborda cuestiones relativas a la protección de datos y la intimidad— continúa puntualizando que, respecto a la existencia de diferentes grados de solidez en las técnicas de anonimización, exhorta a tener en cuenta tres riesgos claves en la anonimización, los cuales son:

- Singularización: la posibilidad de extraer de un conjunto de datos, algunos registros (o todos los registros) que identifican a una persona.
- Vinculabilidad: la capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados, ya sea en la misma base de datos o en dos bases de datos distintas. Si el atacante puede determinar (por ejemplo, mediante un análisis de correlación) que dos registros están asignados al mismo grupo de personas, pero no puede singularizar a las personas en este grupo, entonces la técnica es resistente a la singularización, pero no a la vinculabilidad.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

- Inferencia: la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos.

Cabe mencionar que el Grupo de Trabajo mencionado, en su dictamen 05/2014, habla sobre las técnicas de anonimización, y ofrece un gran catálogo de técnicas en donde sintetiza y hace un nexo causal con la singularización, vinculabilidad e inferencia, que se muestra a continuación:

Tabla 1. Fortalezas y debilidades de técnicas de seudonimización y anonimización

	¿Existe riesgo de singularización?	¿Existe riesgo de vinculabilidad?	¿Existe riesgo de inferencia?
Seudonimización	Sí	Sí	Sí
Adición de ruido	Sí	Puede que no	Puede que no
Sustitución	Sí	Sí	Puede que no
Agregación y anonimato k	No	Sí	Sí
Diversidad l	No	Sí	Puede que no
Privacidad diferencial	Puede que no	Puede que no	Puede que no
Hash/Tokens	Sí	Sí	Puede que no

Fuente: tabla del Grupo de Trabajo del Artículo 29 (2014: 26).

Por otra parte, lo que sí contempla el RGPD son los datos seudonimizados, definiendo éstos como:

> el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. (Artículo 4)

En el caso de México, tales conceptos de anonimización o seudonimización son inexistentes, pero sí se define la palabra disociación, la cual es "el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo" (artículo 3, fracción XIII, LGPDPPSO).

Tal como se ha visto, la legislación mexicana no contempla las palabras seudonimizar o anonimizar, sólo disociar. Es así que, en una interpretación teleológica, podemos encontrar que el legislador mexicano en su

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

exposición de motivos —específicamente en un dictamen de la Cámara de Diputados de México (2010), donde la Comisión de Gobernación aprueba un Proyecto de Decreto que expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares, y realiza otras reformas—, específicamente, en la motivación del principio de proporcionalidad, es claro al decir que: "la aplicación de este principio será que deberá tenderse siempre que sea posible en el tratamiento de los datos a realizar el mismo de forma anonimizada o disociada" (2010: 33). Convirtiendo el proceso de disociación como un proceso de anonimización, pero que esto no exime que estén fuera de la ley, pues siempre es fundamental cumplir con el consentimiento.

Un problema conceptual es que se contemplen como sinónimos el seudonimizar y anonimizar información, con la idea de no caer en la potestad del RGPD, ya que los datos anónimos son excluyentes de este ordenamiento. Por ejemplo, un dato cifrado contiene una clave para descifrarlo, y en sentido estricto cae en la aplicación del RGPD. Es un error pensar que los datos disociados o anonimizados no estén bajo la custodia de la ley, pues pese a que la normativa de protección de datos los deje fuera en *lato sensu*, puede existir el supuesto de una violación de la confidencialidad de las comunicaciones, que pese a que los datos están anonimizados, esto no exime la intervención o intercepción de comunicaciones de manera ilícita.

Antes de concluir respecto al debate entre anonimizar y seudonimizar, debemos detenernos a distinguir lo que son la codificación, el cifrado y el *hash*. Para encontrar las diferencias, me baso en el autor Fugaro (2015: 419), con el propósito de expresar lo siguiente.

En resumen, la codificación es para mantener la usabilidad de los datos, y puede revertirse si se emplea el mismo algoritmo con el que se codificó el contenido, sin necesidad de alguna clave. Algunos ejemplos de codificación son ASCII, UNICODE, codificación de URL y BASE64.

Tabla 2. Ejemplos de tipos de codificación

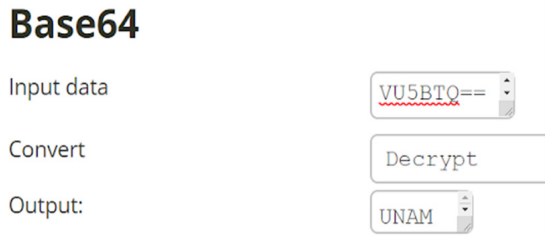
Palabra en texto plano	UNAM
ASCII	085 078 065 077
BASE64	VU5BTQ= =

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Gráfico 12. Ejemplos de decodificación ASCII a texto plano

Fuente: sitio web *http://www.unit-conversion.info/texttools/ascii/*.

Gráfico 13. Ejemplos de decodificación Base64 a texto plano

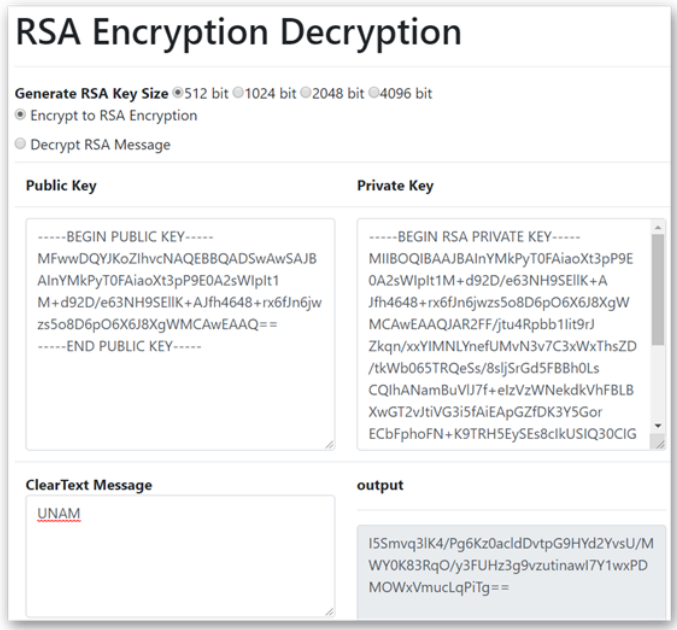


Fuente: sitio web *http://www.unit-conversion.info/texttools/base64/*.

El cifrado es para mantener la confidencialidad de los datos, y se requiere el uso de una clave (secreta) para convertir, o mejor dicho descifrar la información. Como se mencionó, algunos ejemplos son AES, Blowfish o RSA. Cabe destacar que el cifrado es una acción reversible, ya que el titular de la clave puede volver a identificar los datos, o mejor dicho descifrar la información, siendo el cifrado un método seudonimizado y categorizado como un mecanismo de datos identificativos personales, al menos para el titular de la clave capaz de identificar. Si bien se otorga confidencialidad e integridad en la información, no se convierten los datos irreversiblemente anónimos. A continuación, se ejemplifica con RSA (cifrado asimétrico que ya se explicó anteriormente):

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Gráfico 14. Ejemplo de cifrado asimétrico RSA



Fuente: sitio web *https://8gwifi.org/RSAFunctionality?keysize=512*.

Por último, el *hash* es para validar la integridad del contenido, para detectar las modificaciones del mismo a través de cambios en la salida *hash*. Ya se mencionó que, sin importar la cantidad de caracteres, siempre será la misma cantidad de caracteres de salida (dependiendo el método de *hashing*); por ejemplo, en MD5 siempre serán 32 caracteres de salida, mientras que en SHA-256 serán 64 caracteres, esto sin importar la cantidad de caracteres o palabras que se quiera aplicar el *hashing*. De una manera más sencilla, es una función matemática que recibe un valor de entrada que se transforma en un valor de salida de longitud fija.

Tabla 3. Ejemplos de *hashing*

Palabra en texto plano	UNAM
MD5	93908a706f2cd81165fa568701d8fca6
SHA-256	43a171dae6809af0381dbbb73117d20d bf6104d337d5bfacfdf792fb6a234c1c

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Gráfico 15. Se rompe la seguridad de unos *hash* en MD5 y SHA-256

FUENTE: sitio web *https://crackstation.net/*.

Pese a que los ejemplos de *hash crack*, mostrados anteriormente, pudieron romper la seguridad del sistema del *hashing*, y se pudiera argumentar que con una función *hash* se llega a anonimizar la información, y por ende quede fuera del contexto de la legislación especial en protección de datos; no obstante, el Grupo de Trabajo del Artículo 29 (2014: 22) es claro al decir que: "esta función no es reversible, es decir, no existe el riesgo de revertir el resultado, como en el caso del cifrado. Sin embargo, si se conoce el rango de los valores de entrada de la función *hash*, se pueden pasar estos valores por la función a fin de obtener el valor real de un registro determinado".

Además es muy importante mencionar que aplicar la función *hash* no es anonimizar los datos, es seudonimizar, ya que con ataques de fuerza bruta, añadiendo computación cuántica, pueden penetrar la seguridad de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

los sistemas criptográficos. Y es que cada día encontramos tantos problemas de seguridad en protocolos y sistemas criptográficos, que al final ni el cifrado o alguna codificación sirven para que alguien no pueda ser identificado, pues son técnicas para mantener la confidencialidad e integridad de la información según su uso.

En resumen, la anonimización consiste en técnicas que se emplean en datos personales con el objetivo de que se disocien totalmente los datos, sin la posibilidad de identificación de las personas, esto de manera irreversible. La seudonimización hace que los datos personales no se puedan identificar a una persona, sin utilizar información adicional, por lo tanto, es un procedimiento reversible.

Un dato anonimizado es cuando en ningún caso pueda tener un vínculo con un dato que pueda identificar a una persona, haciendo imposible identificar a la persona. Y seudonimización es un procedimiento donde se reemplazan campos de información personal por diversas técnicas, pero se mantienen datos adicionales que pueden identificar a personas.

En conclusión, y como bien lo dice el EU Blockchain Observatory and Forum (2018: 5), actualmente hay intensos debates, pero no consenso sobre lo que se necesita para anonimizar los datos personales hasta el punto en que la salida resultante se pueda almacenar potencialmente en una red *Blockchain*. Por poner un ejemplo, el *hash* de datos no se puede considerar como una técnica de anonimización en muchas situaciones, y sin embargo, hay casos en los que el uso de *hash*, para generar firmas digitales únicas de datos que se almacenan fuera de la cadena, es potencialmente concebible en una *Blockchain*.

V. Soluciones

1. *Derechos ARCO y* Blockchain

Los derechos ARCO son los derechos de acceso, rectificación, cancelación y oposición. Si bien es cierto que la inmutabilidad de la red y transparencia en *lato sensu* son atributos importantes y los mejores aliados para el derecho de acceso a la información, empero, respecto a los derechos de rectificación, cancelación y oposición pudiéramos encontrar conflictos al no poder modificar o borrar información de la red. Dicho lo anterior, a continuación, abordaremos algunas posibles soluciones ante la intersección de esta tecnología *Blockchain* y la protección de datos personales.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

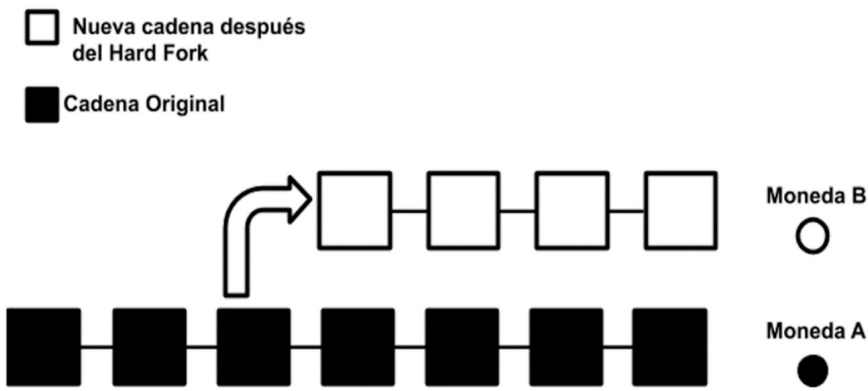
A. *Solución # 1: cambiar los datos y tener bifurcación*

En sentido amplio, los datos no son totalmente inmutables, existe la posibilidad de cambio, ya que los nodos controlan todas las copias de la red, y en el momento en que se cambiaran los datos almacenados, daría como resultado nuevas versiones, llamadas bifurcaciones.

Es decir, también se pudiera dar el caso de modificar la cadena de bloques, pero esto crearía un *Fork* —en español, una bifurcación— donde habría una división en la cadena de bloques, donde existen dos ramas diferentes durante un periodo de tiempo.

La primera es el *Hard Fork*, y se denomina bifurcación dura, porque después de la bifurcación la red no se reconvierte en una sola cadena, las dos cadenas evolucionan independientemente. Los *hard forks* ocurren cuando parte de la red está operando bajo un conjunto diferente de reglas de consenso que el resto de la red. Esto puede ocurrir debido a un error o debido a un cambio deliberado en la implementación de las reglas de consenso (Antonopoulos, 2017: 274).

Gráfico 16. *Hard Fork*



Fuente: gráfico hecho con base en el diagrama realizado por Antonopoulos (2017: 274).

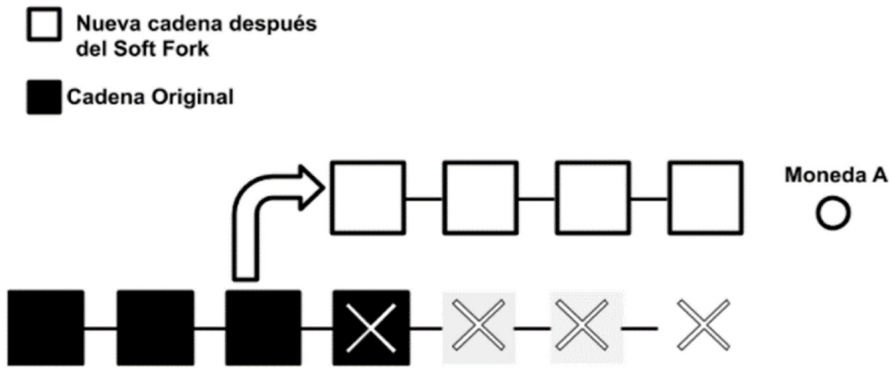
La segunda es el *Soft Fork*, o bifurcación suave, y es un cambio compatible con el avance de las reglas de consenso que permite a los clientes no actualizados continuar operando en consenso con las nuevas reglas. Un aspecto de las bifurcaciones blandas, que no es tan obvio, es que las actua-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

lizaciones de las bifurcaciones blandas sólo pueden usarse para restringir las reglas de consenso, no para ampliarlas (Antonopoulos, 2017: 278).

Es decir, el *Soft Fork* es una divergencia temporal donde los nodos que no han sido actualizados incumplirán algunas de las nuevas reglas, esto porque no las conocen, por lo tanto, se requiere que la mayoría de los nodos mineros actualicen hacia las nuevas reglas.

Gráfico 17. *Soft Fork*



Fuente: gráfico hecho con base en el diagrama realizado por Antonopoulos (2017: 274).

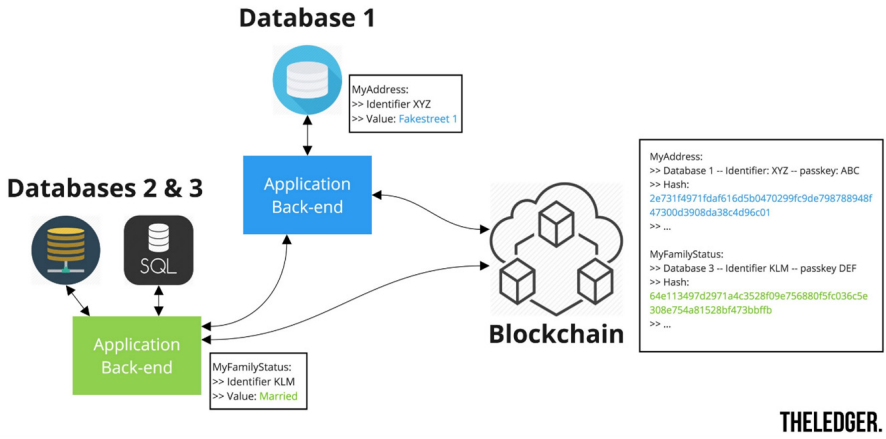
Es decir, con estos *Forks*, que son actualizaciones en el protocolo, se llevaría a la modificación de reglas en menor o mayor grado. Lo que causará que, dependiendo del tipo de modificación que se agregue, los nodos seguirán o no aceptando los nuevos bloques que son generados y agregados a la *Blockchain*. El resultado serán nuevas y diversas cadenas de bloques, cada ocasión que se necesite modificar información.

B. *Solución # 2: almacenar los datos personales fuera de la cadena y* hash *en la cadena*

Como lo menciona Van Humbeeck (2017), en esta posible solución, existe una estructura fuera de la cadena, agregando meramente referencias, identificadores o mejor dicho datos cifrados, convertidos en *hash*, para así comprobar la integridad de los datos personales, cuando sean comparados con los de la red *Blockchain*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Gráfico 18. Solución de almacenamiento de información fuera de línea y los *hash* en la cadena



Fuente: gráfico hecho por Van Humbeeck (2017).

En el gráfico anterior, podemos observar cómo dos entidades diferentes procesan datos en la red *Blockchain*; sin embargo, sólo se almacena en la red el *hash*, o cadena cifrada, para "verificar si estos datos no se han manipulado calculando el *hash* de los datos recuperados y comparándolos con el *hash* proporcionado por la *Blockchain*. Si coinciden, los datos no han sido manipulados" (Van Humbeeck, 2017).

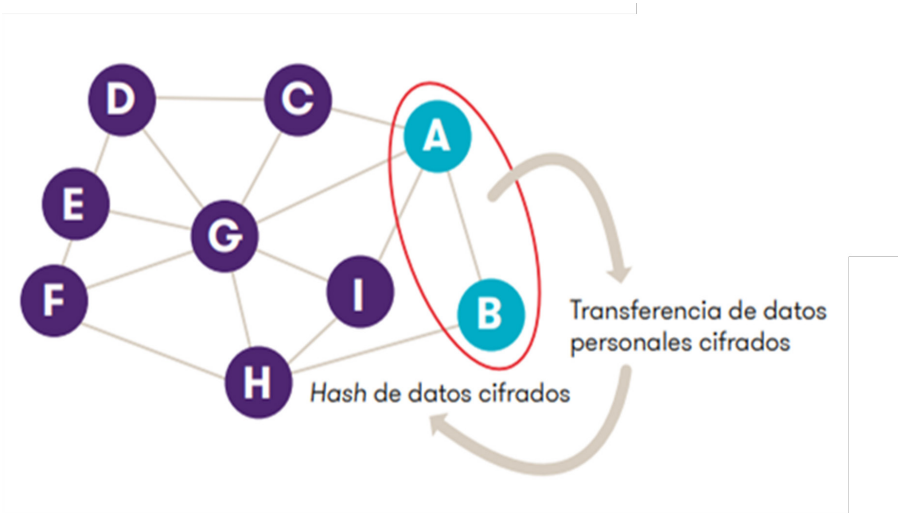
C. *Solución # 3: canal privado de comunicación y los* hash

Otra solución es la que propone la empresa Grant Thornton (2018), que consiste en canales privados con datos cifrados, y cuyo funcionamiento sería:

1) Los nodos A y B crean un canal privado en la *Blockchain*.
2) Los datos personales cifrados se comparten en el canal privado entre A y B.
3) El *hash* de datos cifrados se almacena en la *Blockchain* "común", es decir, el resto de los nodos (C, D, E, F, G, H e I) saben que A y B han compartido información en un momento concreto, pero no pueden visualizar el contenido: sólo ven el *hash* (2018: 06).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Gráfico 19. Transferencia de datos entre canales privados y los datos cifrados al resto de la red



FUENTE: gráfico hecho por Grant Thornton (2018: 6).

Por medio de este mecanismo, en *lato sensu* se podría catalogar como eliminación de los datos, pero en *stricto sensu*, simplemente son anonimizados, porque no se eliminan, sólo quedan los *hash* como datos anónimos, aleatorios, de modo que pasan a ser inteligibles e irrelevantes.

D. *Solución 4: eliminar claves de cifrado*

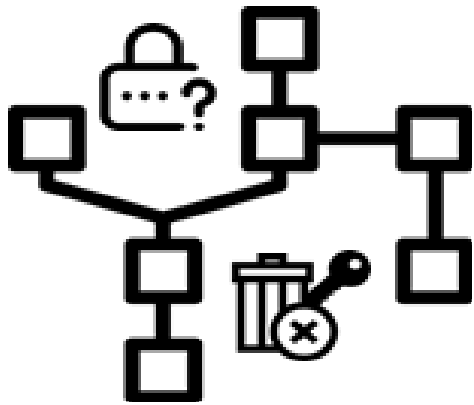
La solución de destruir las claves de cifrado conlleva a que, cuando se pretenda modificar la cadena de bloques, los datos queden inutilizables o ininteligibles: "la eliminación de la clave es una forma efectiva de poner a cero los datos protegidos sin modificar realmente la base de datos. Los datos cifrados no se pueden recuperar si la clave ya no está disponible" (Townsend, 2018). En sentido estricto, no es eliminación, y tendría que considerarse la técnica legislativa de los ordenamientos para conocer si esto cumple como supresión.

Una posible excepción ante esta técnica de borrado es la que contempla la Oficina del Comisionado de Información en Reino Unido, al mencionar que está satisfecha de que la información haya sido puesta fuera de uso, si no se eliminó realmente, siempre que el controlador de datos no

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

pueda, intente o utilice los datos personales, así como no dé acceso a la información a otra organización, y rodee los datos personales de medidas técnicas y de seguridad, así como el compromiso de la eliminación permanente de la información, cuando esto sea posible (2018: 5).

Gráfico 20. Eliminación de la llave privada, para convertir los datos en información ilegible y anonimizada, y cumplir con los derechos de cancelación y oposición



Fuente: gráfico hecho con iconos realizados por Freepik & Becris en *www.flaticon.com*.

En sentido estricto, quizá no se cumpla con el famoso derecho al olvido o derecho de borrado o supresión —como se quiera llamar—, pues acertadamente, como lo indica Ricardo Pazos, la expresión derecho al olvido "evoca un imposible, ya que, en la medida en que todo derecho comporta la correlativa obligación, el derecho al olvido sencillamente no puede existir [...] el derecho al olvido no pretende eliminar información, sino dificultar el acceso a ella" (2015: 6-7), concluyendo que "pese a existir y poder accederse a ella, la información cae en el olvido en la práctica porque se pierde entre el resto de información disponible en internet. Por esta razón se ha propuesto denominar derecho a la oscuridad digital" (2015: 82).

Lo anterior aplica cuando exista una desindexación o anonimización de la información, pues cuando se lleva un derecho de cancelación u oposición ante el garante de la información y se suprima en su totalidad, en sentido estricto sí estaría presente ante un derecho de supresión y no de oscuridad digital.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

2. *Transmisión de datos en redes* Blockchain

Antes de pensar en la transmisión de datos, es necesario precisar algo acerca del controlador de los datos para su tratamiento. En el caso de *Blockchain*, como se ha comentado anteriormente, existen mineros que tienen múltiples funciones; dentro de éstas, se encuentra la de validar las transacciones. Es así que nace la interrogante obligada sobre si ¿los nodos son controladores de datos?, para ello la Commission Nationale de l'Informatique et des Libertés (CNIL) ha expedido un documento referente a soluciones para un uso responsable de la cadena de bloques en el contexto de datos personales, en donde precisa que "los mineros sólo validan las transacciones enviadas por los participantes y no están involucrados en el objeto de estas transacciones: por lo tanto, no definen los propósitos y los medios del tratamiento" (CNIL, 2018b: 2).

Para entender la naturaleza de los mineros, es importante realizar un nexo de clasificación. Se podría definir a tres tipos de nodos como actores en la materia de protección de datos personales, los cuales son:

- "Accesorios", que tienen derecho a leer y guardar una copia de la cadena.
- "Participantes", que tienen derecho a realizar entradas (es decir, realizar una transacción para la que solicitan validación).
- "Mineros", que validan una transacción, y crean bloques en donde aplican las reglas de la cadena de bloques para que la comunidad los "acepte" (CNIL, 2018a).

Otro problema fundamental es la parte del consentimiento, pues cada transmisión es considerada como tratamiento; esto tanto en el RGPD, la LGPDPPSO y la LFPDPPP. En el caso de *Blockchain* privadas podría garantizarse, pero en el caso de las públicas es complejo y debatible, sobre todo si la transmisión de los datos se realiza fuera del país.

Solución # 1. Usuarios responsables de su propia información personal, donde nadie controla o posee sus datos

En el caso de una DLT, al ser un consorcio que decide compartir un registro distribuido, el controlador de los datos deberá ser definido desde un principio. En el caso de que existan varios controladores, se tendrá que llegar a un acuerdo (artículo 26, RGPD).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Por otra parte, en las *Blockchain* públicas, el participante (es decir, la persona que decide registrar datos en una cadena de bloques) puede considerarse un controlador de datos, dado que el participante determina el propósito y medios de procesamiento de datos (CNIL, 2018a); dicho de otra manera, se arribaría a una metamorfosis de los derechos fundamentales de autodeterminación informativa, libertad informática y *habeas data* materializada en algo tangible y real, en donde el responsable del tratamiento sea el mismo titular, otorgándole una total autonomía y control sobre sus datos, convirtiendo los ahora conocidos como datos personales, en datos personales soberanos.

VI. Conclusiones

Durante la presente investigación abordamos diversos puntos de vista referentes a *Blockchain* y su intersección con la transparencia y protección de datos personales. Abordamos diversos enfoques tangibles e interrogantes, en relación a si los datos procesados por esta tecnología son considerados como datos personales, al ser cifrados bajo una función *hash* en consecuencia a la seudonimización o anonimización/disociación. También se llevó a cabo un estudio axiológico de la naturaleza descentralizada y distribuida de *Blockchain* y su posible conflicto con la normatividad, en relación a identificar al controlador de los datos para fines de transferencia y transmisión de información. Así mismo, se abordó el atributo teleológico de la transparencia en las redes *Blockchain* y cómo a pesar de que esto es una ventaja en los sistemas informativos contemporáneos, su mala implementación podría causar ataques que alcanzarían a cumplirse principalmente en redes privadas o DLT, donde se manipule la transparencia de la información al tener una mayoría de mineros en los protocolos de consenso; y por último, se planteó la controversia entre los derechos de rectificación, cancelación y oposición, derecho al olvido, borrado o supresión de la información contra la característica primordial y primigenia de *Blockchain* que es la inmutabilidad de la información y sellado de las transacciones.

En el caso de los controladores o responsables del tratamiento de los datos personales, es necesario previamente identificarlos. Si son varios sujetos, es recomendable formar una persona jurídica, o que cada persona se considere su propio controlador de datos.

No todos los derechos colisionan con la tecnología *Blockchain*; por ejemplo, el derecho de acceso a la información y la portabilidad de los datos son armoniosos al aplicarles dicha tecnología.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Podría considerarse a la *Blockchain* como una revolución o innovación, pero independientemente de esto, las leyes de protección de datos son una evolución, es así que esta intersección entre el derecho y la tecnología deberá darse en armonía y con diálogo.

Con las redes *Blockchain*, se cumple la triada de la seguridad de la información, también conocido como modelo CIA por *confidentiality, integrity, availability*, que en español equivale a confidencialidad, integridad y disponibilidad.

La legislación mexicana en protección de datos personales, así como el RGPD, nacen como una evolución y progresividad de los derechos fundamentales; sin embargo, pareciera paradójico encontrar una intersección entre dos entidades que parecieran polos opuestos complementarios, permitiendo transparencia y portabilidad de los datos eficaz, y por otra parte, complicando la transferencia de información y derecho de rectificación, cancelación y oposición ante el registro. Es necesario crear nuevos instrumentos y mecanismos donde los ciudadanos puedan ser verdaderos dueños de sus datos personales.

Es necesario que, tanto abogados como especialistas en tecnología, deban resolver ciertas interrogantes y disposiciones: primero, al comprender que *Blockchain* es descentralizada y distribuida, habría que identificar a los responsables de la misma, así como de su procesamiento; segundo, las redes son públicas y transparentes, por lo tanto, la información es accesible para todos; y tercero, las redes públicas no son editables ni se puede eliminar la información.

Con la tecnología *Blockchain*, se ha creado un nuevo panorama para el mundo. Tal como lo expresan Don Tapscott y Alex Tapscott: "ahora disponemos de una plataforma verdaderamente igualitaria que hace posibles todas esas apasionantes cosas de las que hablamos […] Cada cual puede ser dueño de su identidad y de sus datos personales" (2017: 23).

VII. Fuentes de información

Agencia Española de Protección de Datos, 2016, *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, disponible en *https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf*.

Antonopoulos, Andreas M., 2017, *Mastering Bitcoin Programming the Open Blockchain*, 2a. ed., Estados Unidos de América, O'Reilly Media, Inc.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Bambara, Joseph J. y Allen, Paul R., 2018, *Blockchain A Practical Guide to Developing Business, Law, and Technology Solutions*, Estados Unidos de América, McGraw-Hill Education.

Bashir, Imran y Narayan, Prusty, 2019, *Advanced Blockchain Development: Build Highly Secure, Decentralized Applications and Conduct Secure Transactions*, Birmingham, Reino Unido, Packt Publishing Ltd.

60 Bashir, Imran, 2017, *Mastering Blockchain*, Birmingham, Reino Unido, Packt Publishing Ltd.

CNIL, 2018a, *Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*, París, disponible en *https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data*.

CNIL, 2018b, *Blockchain Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*, París, disponible en *https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf*.

De Filippi, Primavera y Wright, Aaron, 2018, *Blockchain and the Law: The Rule of Code*, Londres, Harvard University Press.

Erl, Thomas *et al.*, 2015, *Cloud Computing Design Patterns*, Westford, Massachusetts, Prentice Hall.

Eu Blockchain Observatory And Forum, 2018, *Blockchain and the GDPR a Thematic Report Prepared by the European Union Blockchain Observatory and Forum. An Initiative of the European Commission*, disponible en *https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf*.

Ferrajoli, Luigi, 2011, Principia iuris. *Teoría del derecho y de la democracia. 1. Teoría del derecho*, trad. de Perfecto Andrés Ibáñez *et al.*, Madrid, Trotta.

Fugaro, Luigi, 2015, *WildFly Cookbook*, Birmingham, Reino Unido, Packt Publishing Ltd.

Grant Thornton, 2018, *RGPD y Blockchain. Soluciones blockchain para el Reglamento General de Protección de Datos*, Madrid, disponible en *https://www.grantthornton.es/globalassets/1.-member-firms/spain/folletos/rgpd-y-blockchain-final.pdf*.

Grupo de Trabajo del Artículo 29, 2014, Dictamen 05/2014 sobre Técnicas de Anonimización, Adoptado el 10 de Abril de 2014, Bruselas, Bélgica, disponible en *https://gahazas.files.wordpress.com/2018/10/wp216_es_-tc3a9cnicas-de-anonimizacic3b3n.pdf*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Gupta, Rajneesh, 2018, *Hands-On Cybersecurity with Blockchain: Implement DDoS protection, PKI-based identity, 2FA, and DNS security using Blockchain*, Birmingham, Reino Unido, Packt Publishing Ltd.

Humbeeck, Andries van, 2017, "The Blockchain-GDPR Paradox", disponible en *https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047*.

IBM, 2018, *Blockchain and GDPR. How blockchain Could Address Five Areas Associated with GDPR Compliance*, Cambridge, Estados Unidos de América, disponible en *https://www.ibm.com/downloads/cas/2EXR2XYP*.

Information Commissioner's Office, 2018, *Deleting Personal Data Protection Act*, Wilmslow, Reino Unido, disponible en *https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf*.

Llamas C., Jersain Z. y Llamas C., Irving N., 2018, *Internet, ¿arma o herramienta?*, Guadalajara, Jalisco, México, Universidad de Guadalajara, Centro Universitario de Ciencias Sociales y Humanidades, disponible en *http://www.publicaciones.cucsh.udg.mx/kiosko/2018/internet_arma_o_herramienta_Ebook.pdf*.

Luhmann, Niklas, 1998, *Sistemas sociales: lineamientos para una teoría general*, 2a. ed., coord. de Javier Torres Nafarrate, trad. de Silvia Pappe y Brunhilde Erker, Rubí, Barcelona-México-Santafé de Bogotá, Anthropos Editorial-Universidad Iberoamericana-Pontificia Universidad Javeriana, Centro Editorial Javeriano.

McAndrew, Alasdair, 2011, *Introduction to Cryptography with Open-Source Software*, Nueva York, Estados Unidos de América, CRC Press Taylor & Francis Group.

Nakamoto, Satoshi, 2008, "Bitcoin: un sistema de efectivo electrónico usuario-a-usuario", trad. de Ángel León, disponible en *https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf*.

Pazos Castro, Ricardo, 2015, "El mal llamado derecho al olvido en la era de internet", Ministerio de Justicia, Gobierno de España, disponible en *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2689967*.

Quirós, Fernando, 2019, "Advierten que en México debe realizarse un estudio exhaustivo antes de implementar tecnología blockchain para votaciones", *CoinTelegraph en Español*, disponible en *https://es.cointelegraph.com/news/they-warn-that-in-mexico-an-exhaustive-study-must-be-carried-out-before-implementing-blockchain-technology-for-voting*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Swan, Melanie, 2015, *Blockchain: Blueprint for a New Economy*, Estados Unidos de América, O'Reilly Media, Inc.

Tapscott, Don y Tapscott, Alex, 2017, *La revolución blockchain*, trad. de Juan Manuel Salmerón, Barcelona, Deusto.

Townsend, Patrick, 2018, "GDPR Right of Erasure (Right to be Forgotten), and Encryption Key Management", disponible en *https://info.townsendsecurity.com/gdpr-right-erasure-encryption-key-management*.

Yaga, Dylan *et al.*, 2018, *NISTIR 8202 Blockchain Technology Overview*, National Institute of Standards and Technology, U.S. Department of Commerce, disponible en *https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf*.

Zambrano, Raúl, 2017, *Blockchain. Unpacking the Disruptive Potential of Blockchain Technology for Human Development. White Paper*, Ottawa, Canadá, International Development Research Centre.

VIII. Marco jurídico

Cámara de Diputados, 2010, Comisión de Gobernación. Dictamen con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II, del título segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ciudad de México, disponible en *http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf*.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010, México, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017, México, disponible en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*.

Reglamento General de Protección de Datos, 2016, Europa, disponible en *https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&qid=1558482949720&from=EN*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

IX. Glosario

Nodo: es un ordenador conectado a la red *Blockchain*, que por medio del *software* almacena y distribuye en tiempo real una copia actualizada de la cadena de bloques

Hash: función criptográfica. Es un algoritmo matemático que convierte cualquier dato en una nueva serie de caracteres con una longitud fija, sin importar la longitud de los datos a cifrar; es decir, el valor *hash* de saliente será siempre de la misma longitud.

Nonce: número aleatorio, usado una sola ocasión, para autenticar transferencias de datos.

Minero: nodo de la *Blockchain*, encargado de validar las transacciones mediante un mecanismo de consenso.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

LA PROTECCIÓN DE DATOS PERSONALES ANTE EL EJERCICIO DE LOS DERECHOS POLÍTICO-ELECTORALES EN MÉXICO

THE PROTECTION OF PERSONAL DATA BEFORE THE EXERCISE OF POLITICAL-ELECTORAL RIGHTS IN MEXICO

*Hiram Raúl Piña Libien**
*Enrique Uribe Arzate***

RESUMEN. La protección de datos personales en el ámbito político-electoral mexicano se sustenta en un régimen jurídico amplio, que garantiza el registro de los ciudadanos como electores y su derecho a participar como candidato; promueve su libertad individual y voluntad para afiliarse a un partido político, así como brindar su apoyo ciudadano a quienes aspiren a ser candidatos independientes; sin embargo, establece también prohibiciones y sanciones por la dispersión ilegal del padrón electoral. En este texto se exponen los alcances y límites de la legislación mexicana y la jurisprudencia emitida por el Tribunal Electoral del Poder Judicial de la Federación, así como las experiencias derivadas de casos empíricos, con el fin de establecer que los datos personales en materia político-electoral en México posee diferentes grados de protección.

* Doctor en derecho por la Universidad Autónoma del Estado de México (UAEM). Profesor-investigador de tiempo completo en la Facultad de Derecho de la UAEM. *hrpl@hotmail.com*.

** Doctor en derecho por la Universidad Nacional Autónoma de México. Profesor-investigador de tiempo completo en la Facultad de Derecho de la UAEM. Investigador nacional nivel II. *vercingtx@hotmail.com*.

Fecha de recepción: 30 de julio de 2019.
Fecha de dictamen: 26 de agosto de 2019.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

PALABRAS CLAVE. Protección de datos, derechos político-electorales, partido político, padrón electoral, candidaturas independientes, afiliación indebida.

ABSTRACT. The protection of personal data in the Mexican political-electoral field is based on a broad legal regime, which guarantees the registration of citizens as voters and their right to participate as a candidate; promotes their individual freedom and willingness to join a political party, as well as providing their citizen support to those who aspire to be independent candidates; however, it also establishes prohibitions and sanctions for the illegal dispersion of the electoral roll. This text sets out the scope and limits of Mexican legislation and jurisprudence issued by the Electoral Tribunal of the Judicial Branch of the Federation, as well as the experiences derived from empirical cases, establishing that the protection of personal data in political-electoral matters in Mexico has different degrees of protection.

KEYWORDS. Data protection, political-electoral rights, political party, electoral roll, independent candidates, undue affiliation.

I. Introducción

El presente trabajo tiene por objetivo general dilucidar cómo se protegen los datos personales en el ámbito político-electoral en México, cuáles son las vías jurídicas a las que pueden recurrir los ciudadanos mexicanos para proteger sus datos personales relacionados con actividades político-electorales, y qué obligaciones y responsabilidades tienen los distintos actores políticos ante el tratamiento de los datos personales de los ciudadanos.

En esta tesitura, en el primer apartado se establece la relación teórico-conceptual entre los derechos político-electorales y el derecho a la protección de datos personales.

En el apartado segundo analizamos el procedimiento que permite a los ciudadanos mexicanos contar con su credencial para votar con fotografía. El tercero se dedica al procedimiento preelectoral que deben satisfacer los aspirantes a una candidatura independiente para la obtención del apoyo ciudadano.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

El cuarto apartado presenta la obligación de los partidos políticos para abstenerse de afiliar a un ciudadano en contra de su voluntad.

Finalmente, en el quinto apartado, se muestra la responsabilidad de los partidos políticos y sus representantes ante la dispersión ilegal del Padrón Electoral (PE).

II. Los derechos político-electorales *vis a vis* el derecho a la protección de datos personales

Diversos estudios sobre calidad de la ciudadanía en México (INE, 2015; INEGI, 2017; IEEM, 2019) señalan que es un proceso complejo y en construcción. Evidencian que es frágil a consecuencia de la desconfianza que se tiene hacia las autoridades —sean electas o delegadas, del orden federal, estatal o municipal—, y que su actuar está reprobado, debido a malas prácticas electorales (Méndez, 2017) y la prevalencia de la corrupción.

El tratamiento inadecuado de datos personales de los ciudadanos es parte de esos yerros que se gestan en la praxis político-electoral.

Para contextualizar la importancia de nuestro estudio, requerimos de una aproximación teórico-conceptual a los derechos político-electorales y al derecho a la protección de datos personales.

Los derechos civiles, políticos y sociales acuñados en el último tercio del siglo XVIII dieron sustento al Estado moderno, concibiendo una forma de organización de la vida política, económica y social, fundada en los principios de libertad, igualdad y fraternidad.

En oposición a la doctrina del derecho divino, la teoría de la soberanía nacional sustentó la superación de las diferencias políticas y jurídicas entre pueblo y nobles, rebasar la distinción entre gobernantes y gobernados (Duverger, 1970: 25), mediante el establecimiento de una asamblea nacional, la cual funge como un ente de representación social (Sieyès, 1989).

Resultado de ello fue la construcción del Estado liberal, caracterizado por que todos los hombres sin distinción de clase, raza y sexo se encuentran sometidos a un mismo derecho, a un Estado en el que no existen fueros o privilegios, en el que están erradicadas las prebendas.

Esencialmente, los derechos políticos son "una autorización para influir en la constitución de la voluntad estatal; ello significa participar, directa o indirectamente en la producción del orden jurídico, en el que se expresa la 'voluntad estatal'" (Kelsen, 1993: 150).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Desde el punto de vista constitucional, la participación en los asuntos públicos se encuentra sujeta al límite que el ordenamiento jurídico impone a las personas para reconocerles el estatus jurídico de ciudadano, mediante el cumplimiento de una determinada edad biológica.

Para que esa capacidad a participar políticamente se concrete, es preciso que el ordenamiento constitucional reconozca ciertos derechos básicos como votar y ser votado para todos los cargos de elección popular, peticionar y asociarse libremente con fines políticos; así como establecer un conjunto de reglas que den sentido al sistema electoral orientado a la elección y sustitución periódica de los representantes populares.

En una visión de conjunto, los derechos político-electorales, además de sustentar a la ciudadanía como una cualidad individual en la que se relacionan derechos políticos y obligaciones electorales, posibilitan y aseguran a los ciudadanos su participación democrática en la conformación de los poderes públicos.

Acotado el sentido de los derechos político-electorales, procedemos a discurrir sobre la protección de los datos personales.

Partiendo de la consideración de que los riesgos a que se encuentra expuesta la dignidad humana, frente a las diversas técnicas de procesamiento de datos, la información de cualquier persona es tanto un atractivo para quienes acechan las actividades individuales, como un valioso activo para quienes persiguen fines de índole comercial, empresarial o político. En ambos supuestos, se trata de "información cuyo contenido se refiere a cuestiones privadas y cuyo conocimiento general puede ser generador de perjuicio o discriminación" (Pierini *et al*., 1999: 25).

Frente a esas modernas técnicas, juegos de asedio y condicionamiento, así como los incentivos derivados del uso ilícito de información personal, se erige el derecho a la intimidad informática, cuyo fin es el "control efectivo, por uno mismo, de la información que le concierne y de salvaguarda de su intimidad" (Barriuso, 1996: 148).[1]

Algunos doctrinarios atribuyen a la intimidad informática significación como derecho a la autodeterminación informativa: así, para Pérez Luño, es la respuesta del presente al fenómeno de contaminación de las libertades (*Liberties Pollution*), que amenaza con invalidar los logros del progreso tecnológico en los Estados de derecho con mayor desarrollo económico

[1] Una técnica de limitación de la informática se prevé en el artículo 18.4 de la Constitución Española de 1978. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

(1989: 162). De ahí que los bienes jurídicos a tutelar sean la intimidad y la vida privada del individuo frente al poder informático.

Otros autores sustentan un derecho a la libre disposición de datos personales, el cual supone recrear un derecho fundamental que, derivado del derecho a la vida privada del hombre, le permite resolver por sí mismo el tratamiento que quiera asignar a los datos que sobre su persona se almacenen con destinos diferentes (Villanueva y Díaz, 2015: 26).

La protección de datos personales es un derecho que tiene como esencia "dotar a las personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales" (Lucas Murillo, 1990: 25).

Ahora bien, ¿qué son los datos personales? En sentido amplio, son cualquier información concerniente a una persona física identificada o identificable; y en sentido restringido, son aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Dentro de este tipo de informaciones, se sitúan aquellas que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Ante las variadas posibilidades para irrumpir en la intimidad informática de las personas, se precisa la existencia de un mecanismo jurídico para la protección de los datos personales. Tanto la doctrina como algunos textos constitucionales lo identifican como *Habeas Data*. Se trata de "un instrumento para controlar la calidad de ellos, corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su posible transmisión" (Ekmekdjian y Pizzolo, 1996: 23).

El derecho mexicano identifica esta vía de protección con la potestad jurídica que asiste a las personas para poder acceder, rectificar, cancelar u oponerse al tratamiento de sus datos personales, es decir, ejercer los denominados derechos ARCO —previstos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM)—; al igual que el *Habeas Data*, son un mecanismo que "constituye un cauce procesal para salvaguardar la libertad de la persona en la esfera de la informática" (Pérez Luño, 1996: 44).

Tanto el *Habeas Data*, como los derechos ARCO, persiguen

> cinco objetivos principales: *a)* que una persona pueda acceder a la información que sobre ella conste en un registro o banco de datos; *b)* que se actualicen los datos atrasados; *c)* que se rectifiquen los inexactos; *d)* que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

conocimiento por terceros, y *e)* supresión en los procesos de obtención de información del requisito de la llamada información sensible, entre la que cabe mencionar la vida íntima, ideas políticas, religiosas o gremiales (Pierini *et al*., 1999: 16-17).

De lo anterior, podemos establecer una interdependencia entre los derechos político-electorales y la protección jurídica de los datos personales, ya que los derechos para votar, ser votado y de afiliación libre y pacífica para tomar parte en los asuntos políticos, constituyen la base de la vida política y de la participación de la ciudadanía en los asuntos públicos; en tanto que la protección de datos personales se configura como una libertad individual ante el poder informático, consistente en reconocer a las personas el derecho a saber cómo, quién y qué datos se han recabado y obtenido, con qué fin son utilizados, y mediante un mecanismo jurídico de tutela exigir su respeto, prohibir su difusión a terceros para cualquier finalidad, así como para su interconexión o vinculación hacia otros que estén disgregados en otras bases de datos.

En el contexto político-electoral mexicano, esta interdependencia cobra relevancia ante el reporte del Instituto Nacional Electoral (INE), que al 16 de agosto de 2019 contabilizó el registro de 90 230 105 ciudadanos mexicanos inscritos en el PE, de los cuales 89 229 360 cuentan con su credencial para votar con fotografía, situación que les posibilita estar registrados en la Lista Nominal de Electores (LNE).

III. El registro ciudadano como elector

En atención al contenido de las fracciones I y II del artículo 35 de la CPEUM, es derecho de los ciudadanos votar en las elecciones populares y poder ser votados para todos los cargos de elección popular. Para esto último, se deberá cumplir con las calidades, requisitos, condiciones y términos que para cada caso establezca la ley, así como solicitar su registro ante la autoridad electoral como candidato postulado a través de un partido político o de forma independiente.

A fin de hacer operativo el ejercicio de estos derechos, el artículo 54 de la Ley General de Instituciones y Procedimientos Electorales (LGIPE) confiere, entre otras atribuciones, a la Dirección Ejecutiva del Registro Federal de Electores (DERFE), las de formar el PE, mediante una técnica

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

censal, y expedir la credencial para votar,[2] proceso que es revisado y actualizado anualmente.

Los documentos, datos e informes que los ciudadanos proporcionan al Registro Federal de Electores (RFE), en cumplimiento de las obligaciones que les impone la CPEUM y la LGIPE, tienen el carácter estricto de confidenciales y no pueden comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en los que el INE fuese parte, para cumplir con las obligaciones previstas por la ley y por la Ley General de Población en lo referente al Registro Nacional Ciudadano o por mandato de juez competente.

Para la incorporación de los ciudadanos al PE, es necesario presentar una solicitud individual ante las oficinas de la DERFE correspondiente a su domicilio, en la que, previa identificación del compareciente, se asientan los siguientes datos: *a)* apellido paterno, apellido materno y nombre completo; *b)* lugar y fecha de nacimiento. En el caso de los ciudadanos mexicanos residentes en el extranjero, deberán acreditar la entidad federativa correspondiente a su lugar de nacimiento. Aquellos que nacieron en el extranjero y nunca han vivido en territorio nacional, deberán acreditar la entidad federativa de nacimiento del progenitor mexicano. Cuando ambos progenitores sean mexicanos, señalar la de su elección; *c)* edad y sexo; *d)* domicilio actual y tiempo de residencia; *e)* ocupación; *f)* en su caso, el número y fecha del certificado de naturalización, y *g)* firma y, en su caso, huellas dactilares y fotografía del solicitante.

El personal administrativo encargado de la inscripción asienta los siguientes datos: *a)* entidad federativa, municipio y localidad donde se realiza la inscripción; *b)* distrito electoral federal y sección electoral correspondiente al domicilio, y *c)* fecha de la solicitud de inscripción.

Una vez que los ciudadanos se han inscrito e incorporado en el PE, la autoridad electoral expide la credencial para votar con fotografía, la que, al ser entregada a su recipiendario, le habilita para participar en la toma de decisiones político-electorales. Sin embargo, la credencial para votar con fotografía, desde su instauración en 1992, ha adquirido un sentido metae-

[2] La credencial para votar con fotografía tiene como características en su modelo, diseño y contenido, las que fueran aprobadas por el Consejo General del Instituto Federal Electoral en su sesión ordinaria del 3 de julio de 1992 y publicadas en el *Diario Oficial de la Federación* de 20 de julio de 1992. Con el propósito de modernizar tecnológicamente la expedición de la credencial para votar con fotografía, incorporarle medidas de seguridad, adecuarla a las reformas constitucionales y legales en materia político-electoral, posibilitar su uso como medio de identificación ciudadana y el ejercicio de otros derechos fundamentales, ha tenido actualizaciones y modificaciones en 2001, 2008, 2012, 2013 y 2015.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

lectoral, pues es empleada como documento de identificación personal para la realización de todo tipo de trámites, tanto públicos como privados.

La expedición de la credencial para votar con fotografía conforma el PE, una base de datos en la que se encuentran registrados todos los ciudadanos que han solicitado su inscripción como electores, sin embargo, para que el ciudadano pueda participar en los procesos electorales, es indispensable que acuda a recogerla, para con ello aparecer en la LNE del PE.

Una vez que el ciudadano ha recibido su credencial para votar con fotografía, tiene la posibilidad de actualizar, rectificar y cancelar los datos que se tengan sobre él.

La actualización del PE se efectúa mediante una campaña en la que se convoca y orienta a los ciudadanos para la incorporación de aquellos que lo hagan por primera vez, a quienes no lo hicieron durante la aplicación de la técnica censal y aquellos que hubiesen alcanzado la ciudadanía con posterioridad a su aplicación; igualmente se convoca a los ciudadanos que no hubieren notificado su cambio de domicilio, a los que no estén registrados en el PE, a los que hubieren extraviado su credencial para votar y a los suspendidos en sus derechos políticos que hayan sido rehabilitados.

En caso de que la actualización o alta sea por cambio de domicilio, deberá ser exhibida al momento de la entrega de la nueva credencial para votar con fotografía, la correspondiente al domicilio anterior, con lo cual se procederá a la cancelación de la primera inscripción y la inmediata destrucción del plástico antiguo. En caso de extravío, deberán ser aportados los datos necesarios.

La expedición de la credencial puede ser solicitada en el año de la elección por aquellos ciudadanos que, habiendo cumplido con los requisitos y trámites correspondientes, no la hubiesen obtenido oportunamente, promoviendo la instancia administrativa correspondiente, hasta el día último de enero.

Para los casos de los ciudadanos que hayan obtenido en tiempo y forma su credencial para votar con fotografía, pero no se encuentran incluidos en la LNE de la sección correspondiente a su domicilio o consideran haber sido indebidamente excluidos de la LNE, podrán presentar solicitud de rectificación a más tardar el día 14 de marzo.

En estos casos, el ciudadano tendrá que requisitar el formato de solicitud que para tal efecto ponga a disposición el RFE.

Se trata de un trámite de carácter administrativo, pues quien conoce sobre la procedencia para la expedición o rectificación de la credencial, es la oficina ante la cual se haya solicitado, misma que deberá resolver dentro del término de veinte días naturales.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

En caso de que esta instancia de carácter administrativo declare improcedente la obtención o rectificación de la credencial, o en el supuesto de que la respuesta no sea en el tiempo legal establecido, la resolución correspondiente podrá impugnarse ante el Tribunal Electoral del Poder Judicial de la Federación (TEPJF), es decir, promover la impugnación prevista en la fracción V del artículo 99 de la CPEUM, identificada como juicio para la protección de los derechos político-electorales del ciudadano; el cual se constituye como el mecanismo de defensa que los ciudadanos mexicanos pueden ejercer en contra de actos y resoluciones que violen sus derechos para votar, ser votado y de afiliación libre y pacífica para tomar parte en los asuntos políticos del país.

Este juicio procede en contra de diversos actos de las autoridades electorales. Entre los que interesan, para efectos de este trabajo, son los contenidos en los incisos a) al c) del apartado 1 del artículo 80 de la Ley General del Sistema de Medios de Impugnación en Materia Electoral (LGSMIME), en los que se prevé:

a) Habiendo cumplido con los requisitos y trámites correspondientes, no hubiere obtenido oportunamente el documento que exija la ley electoral respectiva para ejercer el voto.
b) Habiendo obtenido oportunamente el documento a que se refiere el inciso anterior no aparezca incluido en la LNE de la sección correspondiente a su domicilio.
c) Considere haber sido indebidamente excluido de la LNE de la sección correspondiente a su domicilio.

Este juicio para la defensa de los derechos político-electorales de los ciudadanos exige como requisito *sine qua non*, para su trámite, que el actor previamente agote las instancias jurídicas previas.

En este tipo de juicios, las sentencias que se pronuncien son definitivas e inatacables y tienen por efecto confirmar, revocar o modificar el acto o resolución impugnado. En caso de que se revoque o modifique el acto o resolución, se restituirá al promovente el derecho político-electoral que se le haya violentado.

Cuando la sentencia sea favorable al quejoso y se haya reclamado la violación de alguno de los derechos esgrimidos en los incisos a) al c), tendrá por efectos obligar a la autoridad responsable a la restitución; empero, si ésta se halla impedida por razón de los plazos legales o por imposibilidad técnica o material, y por ello no se pueda incluir debidamente al ciuda-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

dano en la LNE correspondiente a la sección de su domicilio, o expedirle el documento que exija la ley electoral para poder sufragar, bastará con la exhibición de la copia certificada de los puntos resolutivos del fallo, así como de una identificación para que los funcionarios electorales permitan al ciudadano el ejercicio de su derecho al voto el día de la jornada electoral, en la mesa de casilla que corresponda a su domicilio o, en su caso, en una casilla especial.

El juicio para la protección de los derechos político-electorales del ciudadano posee una fuerza restitutoria para que pueda participar activamente en los comicios.

La presentación y resolución de este tipo de juicios ha conducido a que el TEPJF, en concordancia con la reforma constitucional de 2011 en materia de derechos humanos, no solamente interprete la constitucionalidad de los actos de las autoridades electorales, sino también realice una interpretación de la convencionalidad de los derechos que deben ser garantizados ante el tratamiento de los datos personales con fines electorales.

En este tipo de ejercicios interpretativos, destacan los alcances y límites establecidos en la tesis XXXVII/2009, a través de la cual el TEPJF ha establecido que la protección de datos en materia electoral no discrepa del ejercicio de los derechos político-electorales y la transferencia legítima de datos personales entre dependencias gubernamentales.

Es criterio del TEPJF que la expedición y entrega de la credencial para votar con fotografía no se encuentra condicionada a que el ciudadano autorice la incorporación de la clave poblacional, cuya procedencia es una base de datos gubernamental en posesión de una autoridad distinta a la electoral, puesto que esta última se encuentra compelida a cumplir con un mandato establecido en la ley, por lo cual debe insertarla a pesar de que el ciudadano se oponga, pues de no hacerse dicha inserción se podría afectar el derecho de voto.

Por otra parte, en la tesis XXXV/2015 se establece un derecho de acceso irrestricto a la información confidencial que obra en poder de las autoridades electorales a favor de los representantes de los partidos políticos, siempre y cuando se realice para el efecto exclusivo del ejercicio de las atribuciones que legalmente tienen encomendadas, sin reproducirla, en cualquier forma, ni usarla para otros fines, so pena de incurrir en responsabilidad administrativa, civil, penal o política, según corresponda.

Finalmente, en la jurisprudencia 13/2016, el TEPJF ha establecido que es obligación de los órganos del Estado adoptar medidas tendentes a hacer efectiva la tutela y reserva de la información concerniente a la vida privada de las personas, quienes de forma proporcional deberán tener ga-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

rantías respecto de la confiabilidad en el manejo y cuidado de sus referencias concernientes al ámbito de su vida privada.

IV. El tratamiento de datos personales en las candidaturas independientes

Un elemento que caracteriza al Estado constitucional es la existencia de elecciones democráticas, plurales y participativas, en donde el derecho a votar y ser votado para todos los cargos de elección popular se constituye en un mecanismo insustituible de participación ciudadana en la toma de decisiones colectivas y populares.

En la construcción de este arquetipo, los ciudadanos mexicanos tenemos reconocido el derecho a votar y ser votados para todos los cargos de elección popular, debiendo para ello cumplir con las calidades que para cada caso establezca la ley.

En la genética-teleológica de las instituciones constitucionales y democráticas en México, este derecho registra una importante evolución ligada a la igualdad formal de la mujer y el varón ante la ley, como es el caso del reconocimiento del voto femenino en 1953.

A partir de la reforma constitucional introducida en agosto de 2012, el derecho a ser votado se potencializó mediante la incorporación de la figura de candidatura independiente, para posibilitar que los ciudadanos podamos contender en las elecciones federales, estatales o municipales, sin la necesidad de contar con el respaldo de un partido político, previa satisfacción de los requisitos, condiciones y términos que al efecto se establezcan.

En el constitucionalismo mexicano, está figura de participación político-democrática se traduce en la posibilidad de que en la boleta electoral los electores podamos elegir entre candidatos postulados por partidos políticos y candidatos ciudadanos que cuenten con el apoyo de otros ciudadanos. En otras palabras, la candidatura independiente trae consigo la supresión del monopolio de la postulación y registro de candidatos ante la autoridad electoral por parte de los partidos políticos.

En la geopolítica mexicana este derecho a postularse mediante el apoyo de otros ciudadanos encuentra antecedente en Tamaulipas (1998) a nivel municipal, en Michoacán y en el Estado de México (2001 y 2003), respectivamente; en Yucatán (2006) se reconoció la figura de candidatura independiente a nivel constitucional y legislativo; y en Sonora (2008) a través de su ley electoral; así como en la sentencia de la Comisión Interamericana de Derechos Humanos del 6 de agosto de 2008, a través de la

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

cual resolvió el *Caso Castañeda Gutman vs. Estados Unidos Mexicanos* por la violación de los derechos de participación política.

Con el objeto de que la reforma constitucional de 2012 resultara operativa y ante la necesidad de establecer condiciones de equidad en las contiendas electorales entre partidos políticos y candidatos independientes, en 2014 se reformaron los artículos 41 y 116 constitucionales para que los candidatos independientes accedan a prerrogativas para las campañas electorales, lo cual se tradujo en garantizar su derecho al financiamiento público y el acceso a la radio y la televisión.[3]

Ante este contexto, fue imprescindible actualizar el marco reglamentario del sistema electoral mediante la aprobación de la LGIPE, la Ley General de Partidos Políticos y la Ley General en Materia de Delitos Electorales (LGMDE), así como la reforma de la LGSMIME, cuerpos normativos que constituyen los engranajes para la realización de elecciones democráticas, justas, transparentes, participativas y competitivas.

Es preciso señalar que la LGIPE define al candidato independiente como el ciudadano que obtenga por parte de la autoridad electoral el acuerdo de registro, habiendo cumplido los requisitos que para tal efecto establece la ley, es decir, que para ostentar tal calidad será preciso cumplir con ciertas condiciones y términos legales para participar en la elección de presidente de los Estados Unidos Mexicanos, así como de diputados y senadores del Congreso de la Unión por el principio de mayoría relativa.

En la LGIPE se establece que la selección de un candidato independiente se desarrollará mediante el desahogo de las fases de convocatoria, actos previos al registro, obtención del apoyo ciudadano y registro.

Para la realización de la primera fase del proceso —selección de candidatos independientes— el Consejo General del INE debe emitir una convocatoria dirigida a los ciudadanos mexicanos que se encuentren interesados y aspiren a postularse para ocupar el cargo de presidente de los Estados Unidos Mexicanos, diputado o senador del Congreso de la Unión por el principio de mayoría relativa, según sea el caso, señalando en la misma los requisitos que se deben cumplir, la documentación comprobatoria requerida, los plazos para recabar el apoyo ciudadano correspondiente, los topes de gastos que pueden erogar y los formatos para ello.

[3] La figura de candidatura independiente se introdujo con la reforma constitucional del 9 de agosto de 2012, fue en las elecciones del 7 de junio de 2015 que, como consecuencia de la reforma constitucional en materia político-electoral de 2014 y con la expedición de la LGIPE, se materializó tanto a nivel federal como local la posibilidad de acceder a cargos públicos a través de esta vía.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

En esta primera fase, los ciudadanos que deseen participar en la correspondiente convocatoria deberán manifestar ante las autoridades electorales competentes su intención, las cuales la recibirán y expedirán la constancia de aspirante a quienes satisfagan los requisitos previstos en los artículos 55, 58 y 82 de la CPEUM, según el cargo de que se trate, así como los establecidos en los artículos 10 y 383 de la LGIPE.

Tomando como ejemplo la convocatoria emitida para el proceso electoral federal 2017-2018, el Consejo General del INE requirió a los ciudadanos interesados en participar para que, además, exhibieran los siguientes documentos: copia simple legible del anverso y reverso de la credencial para votar del ciudadano interesado, del representante legal y del encargado de la administración de los recursos; carta firmada por la o el aspirante en la que acepta notificaciones vía correo electrónico sobre la utilización de la aplicación informática, así como para recibir información sobre el apoyo ciudadano entregado al Instituto a través de dicha aplicación; y, opcionalmente, podrá entregar el emblema que le distinga durante la etapa para recabar el apoyo de la ciudadanía.

Los ciudadanos interesados en participar en un proceso electoral federal como candidato independiente, en este punto, adquieren el estatus jurídico-administrativo de aspirante a candidato independiente.

Una vez que las autoridades electorales competentes han expedido la constancia que acredita que un ciudadano asume la calidad de aspirante a candidato independiente, se apertura la fase correspondiente a la obtención del apoyo ciudadano, misma que inicia al día siguiente de haberse recibido el documento de acreditación.

Esta fase consiste en la realización de actos tendentes a legitimar la aspiración ciudadana mediante la celebración de reuniones públicas, asambleas, marchas y todas aquellas actividades dirigidas a la ciudadanía en general —excepto la contratación de propaganda o cualquier otra forma de promoción personal en radio y televisión—, fundamentalmente, para que el aspirante a candidato independiente pueda recabar la firma del mínimo de ciudadanos inscritos en la LNE que la LGIPE exige.

Para recabar la firma de los ciudadanos inscritos en la LNE, es preciso que el respaldo ciudadano sea plasmado en una cédula de apoyo que contenga el nombre, firma y clave de elector o el número identificador al reverso de la credencial para votar con fotografía derivado del reconocimiento óptico de caracteres de la credencial para votar con fotografía vigente de cada uno de los ciudadanos que manifiestan el apoyo en el porcentaje requerido.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Una vez que los aspirantes satisfacen, dentro de los plazos establecidos, los porcentajes de integración de las cédulas de respaldo correspondientes en cada caso, dentro de los tres días subsecuentes, las autoridades electorales competentes deben dar a conocer los nombres de los candidatos o fórmulas registradas y de aquellos que no cumplieron con los requisitos. De esto último deviene que aquellos que cumplan con los requisitos legales, documentales, financieros, fiscales y de apoyo ciudadano, serán registrados como candidatos independientes y tendrán por tanto derecho a las prerrogativas que la ley electoral confiere.

Bajo estas premisas, en el marco del proceso electoral federal 2017-2018, el Consejo General del INE expidió el Acuerdo INE/CG426/2017 por el cual emitió la convocatoria para el registro de candidaturas independientes a la presidencia de la República, senadurías o diputaciones federales por el principio de mayoría relativa, en la que además de establecer los requisitos de elegibilidad anteriormente referenciados, en el considerando 56 dispuso que los datos personales de los aspirantes, de los candidatos independientes, así como de los ciudadanos que los respalden, se encuentran protegidos conforme a la legislación aplicable en materia de transparencia y acceso a la información, por lo que son información confidencial que no puede otorgarse a persona distinta que su titular, a menos que exista una autorización expresa de éste. En tal virtud, los servidores públicos de este Instituto que intervengan en el tratamiento de datos personales, los aspirantes, así como los auxiliares/gestores que éstos designen, deberán garantizar la protección en el manejo de dicha información, por lo que no podrá ser comunicada salvo en los casos previstos por la ley. Asimismo, en el tratamiento de datos personales, los servidores públicos de este Instituto deberán observar los principios de licitud, calidad de los datos, información al titular, consentimiento, seguridad, confidencialidad y finalidad para la que fueron recabados.

De lo anterior se aduce que para la autoridad electoral nacional existen tres grados de protección de los datos personales, constituidos de la siguiente manera:

- Grado 1. Aquellos considerados como información confidencial en términos de la legislación aplicable en materia de transparencia y acceso a la información (los relativos a las y los aspirantes, de los candidatos independientes y aquellos de los ciudadanos que los respalden), y que el INE debe salvaguardar en términos de las obligaciones de transparencia y acceso a la información pública que la ley le impone como sujeto obligado.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

- Grado 2. Aquellos datos personales que son tratados por los servidores públicos del INE, los aspirantes a candidato independiente, así como los auxiliares/gestores que éstos designen para la obtención del apoyo ciudadano, quienes además de garantizar la protección en el manejo de dicha información, no podrán comunicarla salvo en los casos previstos por la ley.
- Grado 3. El tratamiento de datos personales que efectúen los servidores públicos del INE, quienes deberán observar los principios establecidos en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO) y el Reglamento del INE en materia de protección de datos personales.

Regresando al estatus jurídico-administrativo de aspirante que se concede a las personas que desean ser candidato independiente, vale decir que la LGIPE les impone una serie de obligaciones, entre las que destaca, abstenerse de realizar por sí o por interpósita persona, actos de presión o coacción para obtener el apoyo ciudadano, circunstancia que no riñe de ninguna manera con la labor para obtener de forma legítima la obtención del apoyo ciudadano requerido para cada caso.

Como puede observarse, la LGIPE no obliga a los aspirantes a candidato independiente para observar los principios rectores de la protección de datos personales cuando se encuentren en la etapa de obtención del apoyo ciudadano, ni los refiere a la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).

Ante tal incongruencia jurídica, con el objeto de verificar el porcentaje de apoyo ciudadano que se requirió para el registro de candidaturas independientes, el Consejo General del INE expidió el Acuerdo INE/CG387/2017 por el que se emitieron los Lineamientos para la Verificación del Porcentaje de Apoyo Ciudadano que se Requiere para el Registro de Candidaturas Independientes a Cargos Federales de Elección Popular para el Proceso Electoral Federal 2017-2018.

Dicho acuerdo, en concordancia con lo dispuesto en el Reglamento de Elecciones, y a fin de dar certeza al proceso de verificación de que se haya reunido el porcentaje de apoyo ciudadano requerido, según el tipo de elección, establece un procedimiento técnico-jurídico priorizado por la utilización de medidas tecnológicas avanzadas.

En este sentido, el INE desarrolló una aplicación móvil para recabar el apoyo ciudadano, misma que permitió a los aspirantes a candidaturas independientes a cargos federales de elección popular recabar la información de las personas que respaldaron su candidatura, sin la utilización de papel

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

para la elaboración de cédulas de respaldo o para fotocopiar la credencial para votar. Además, el objetivo de esta herramienta era facilitar el conocimiento a la brevedad de la situación registral en LNE de dichas personas, generar reportes para verificar el número de apoyos ciudadanos recibidos por los aspirantes, otorgar a la autoridad certeza sobre la autenticidad del apoyo ciudadano presentado por cada aspirante, evitar el error humano en el procedimiento de captura de información, garantizar la protección de datos personales y reducir los tiempos para la verificación del porcentaje de apoyo ciudadano.

La aplicación desarrollada por el INE tuvo por objeto permitir a los aspirantes a candidato independiente, y a quienes les auxiliaron en la tarea de recabar el apoyo ciudadano, capturar el anverso y reverso de la credencial para votar; efectuar un proceso de reconocimiento óptico de caracteres del nombre y clave de elector; verificar los datos; opcionalmente, tomar una fotografía del ciudadano, obtener su firma, y finalmente, realizar el cifrado y envío telemático de información.

Con posterioridad, a fin de asegurar que se cumplan los requisitos legales establecidos para brindar un apoyo ciudadano y verificar la correspondencia entre los datos del formulario y aquéllos contenidos en la imagen de la credencial para votar, a través de una revisión minuciosa, el INE a través de un verificador llevó a cabo la revisión uno a uno de los registros, para constatar que exista una imagen digital de la credencial para votar original emitida por el Instituto por el anverso y el reverso, la firma de la o el ciudadano, y que esos datos sean idénticos a los mostrados en la captura de la aplicación.

De acuerdo con la estadística del proceso electoral federal 2017-2018, 87 ciudadanos manifestaron al INE su intención de ser candidato independiente para ocupar el cargo de presidente de los Estados Unidos Mexicanos, de los cuales, 39 no cumplieron los requisitos legales exigidos; en consecuencia, 48 aspirantes estuvieron en condiciones de iniciar la captación de apoyo ciudadano, es decir, de recabar los datos personales de quienes congeniaran con su aspiración político-electoral. De esos 48 aspirantes, 2 ciudadanos presentaron su renuncia al proceso, y quedaron en consecuencia 46 aspirantes en aptitud de captar el apoyo ciudadano. De esos 46 aspirantes, 43 no alcanzaron el umbral de apoyo requerido, y solamente 3 ciudadanos alcanzaron el umbral y la distribución geográfica mínima de apoyos. De esos 3 ciudadanos, uno no cumplió por casos de simulación de la credencial para votar con fotografía, otro no cumplió por presentar fotocopias, y el último cumplió con lo dispuesto en el artículo 371, numeral 1 de la LGIPE (Véase tabla 1 en la siguiente página).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Tabla 1

-Etapa	Total
Manifestaciones de intención	**87**
No cumplieron con los requisitos exigidos	- 39
Aspirantes al iniciar la captación de apoyo	**48**
Renuncias presentadas durante el proceso	- 2
Aspirantes con proceso vigente durante la captación de apoyo	**46**
Aspirantes que preliminarmente NO alcanzaron el umbral	- 43
Aspirantes que preliminarmente alcanzaron el umbral y la distribución geográfica mínima de los apoyos	**3**
Aspirantes que no cumplieron por casos de simulación de la Credencial para Votar	- 1
Aspirantes que no cumplieron por fotocopias presentadas	- 1
Aspirantes que no cumplieron al eliminar DUPLICADOS con otros aspirantes	**- N/A**
Aspirantes que cumplieron con lo dispuesto en el art. 371, numeral 1 de la LGIPE	**1**

Fuente: Dictamen INE/CG269/2018.

Tabla 2

NÚM.	ASPIRANTE	APOYO RECIBIDO a través de la APP (total)	INVÁLIDOS (TOTAL)				
			Simulación de la Credencial para Votar	Fotocopia de la Credencial para Votar	Documento inválido	Inválidos	Porcentaje de inválidos respecto a los apoyos revisados
1	JAIME HELIODORO RODRÍGUEZ CALDERÓN	1,990,809	158,532	205,721	23,644	387,897	**32.46%**
2	ARMANDO RÍOS PITER	1,623,271	811,969	88,183	6,265	906,417	**85.58%**
3	MARGARITA ESTER ZAVALA GÓMEZ DEL CAMPO	1,568,665	432	212,198	6,714	219,344	**20.29%**

Fuente: Dictamen INE/CG269/2018.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Lo anterior se debió a que la autoridad electoral, además de observar los supuestos de invalidez de cédulas de apoyo previstos en el artículo 385, párrafo 2 de la LGIPE, detectó constantes y reiteradas inconsistencias o irregularidades durante el proceso de revisión de los expedientes electrónicos, entre los que destacaron: entrega de fotografía de fotocopias de credencial para votar; simulación de la credencial para votar; ausencia de firma; captura de la imagen de dos anversos o dos reversos de la credencial para votar; captura de la imagen de anverso y reverso de dos distintas credenciales para votar; varios registros con la misma credencial para votar y con diferentes claves de elector; imágenes ilegibles; fotografía de documentos distintos a la credencial para votar, imagen de una credencial para votar tomada de una pantalla o monitor (Véase tabla 2 en la anterior página).

Pese a la existencia de inconsistencias o irregularidades durante el proceso de revisión de los expedientes electrónicos, el INE determinó otorgar registro como candidata independiente a la ciudadana Margarita Ester Zavala Gómez del Campo.

Sin embargo, el aspirante Jaime Heliodoro Rodríguez Calderón promovió juicios para la protección de los derechos político-electorales del ciudadano, con el objeto de impugnar los acuerdos generales INE/CG269/2018 e INE/CG295/2018 emitidos por el Consejo General del INE, el 23 y 29 de marzo de 2018, respectivamente. En virtud del primero, se aprobó el dictamen sobre el cumplimiento del porcentaje de apoyo ciudadano requerido para el registro de candidaturas independientes a la Presidencia de la República en el proceso electoral federal 2017-2018, resolviéndose por incumplido dicho requisito para el actor; y, en el segundo, se le negó la solicitud de registro a dicha candidatura, como consecuencia de lo determinado en el primer dictamen.

La Sala Superior del TEPJF, en su sesión celebrada el 9 de abril de 2018, al resolver los juicios SUP-JDC-186/2018 y su acumulado SUP-JDC-201/2018, determinó, además de revocar los actos controvertidos, tener por acreditado el requisito consistente en haber reunido el porcentaje de apoyo ciudadano requerido para la candidatura como candidato independiente a la elección de presidente de la República, por lo que en consecuencia, ordenó al INE emitir un nuevo acuerdo en el que se tuviera que el actor cumplió el requisito del umbral necesario de apoyo ciudadano para la candidatura a la que aspiraba, y en consecuencia se le expidiera el correspondiente registro.

En este punto de análisis, se advierte una colisión entre lo señalado en el considerando 56 del Acuerdo General INE/CG426/2017, respecto de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

los datos personales de los ciudadanos que otorguen su respaldo a quienes aspiren a ser candidatos independientes, y el punto tercero del Acuerdo General INE/CG269/2018, por el cual se ordenó dar vista a la Unidad Técnica de lo Contencioso Electoral de la Secretaría Ejecutiva del INE, así como a la Fiscalía Especializada para la Atención de Delitos Electorales, por contravenirse disposiciones previstas en el Código Penal Federal.

Se aduce lo anterior en razón de que en el primer acuerdo se señala que los datos personales que respalden a los candidatos independientes se encuentran protegidos conforme a la legislación aplicable en materia de transparencia y acceso a la información, por lo que son información confidencial que no puede otorgarse a persona distinta que su titular, a menos que exista una autorización expresa de éste. En tal virtud, los aspirantes, así como los auxiliares/gestores que éstos designen, deberán garantizar la protección en el manejo de dicha información, por lo que no podrá ser comunicada salvo en los casos previstos por la ley; mientras que, en el segundo acuerdo, se advirtió que en la etapa de verificación del porcentaje de apoyo ciudadano se detectaron registros con inconsistencias, entre los que destacan el uso de fotografías que no correspondían a la persona que otorgaba el apoyo, uso de fotocopias de la credencial para votar cuya procedencia se atribuía a la realización de trámites administrativos ante dependencias gubernamentales y simulaciones de la credencial para votar.

La autoridad electoral evidenció que el aspirante a candidato independiente y/o sus gestores/auxiliares, además de violentar las reglas electorales, infringieron las disposiciones legales que tipifican como delito el uso indebido de datos personales, como es el caso de lo previsto en la fracción III del artículo 406 del Código Penal Federal, en el que se establece la imposición de 100 a 200 días multa y prisión de uno a seis años, al funcionario partidista o al candidato que sustraiga, destruya, altere o haga uso indebido de documentos o materiales electorales; así como también lo previsto en la fracción II del artículo 409 del citado ordenamiento, en el que se establece la imposición de 20 a 100 días multa y prisión de tres meses a cinco años, a quien altere en cualquier forma, sustituya, destruya o haga un uso indebido del documento que acredita la ciudadanía.

Debe advertirse que la LFPDPPP establece *in genere* que son sujetos regulados por sus disposiciones los particulares, sean personas físicas o morales de carácter privado, que lleven a cabo el tratamiento de datos personales, es decir, dicha ley es aplicable a cualquier persona que obtenga, recolecte, use, acceda, maneje, aproveche, transfiera, disponga, divulgue o almacene datos personales por cualquier medio. Sin embargo, las conductas delictivas que en materia de tratamiento indebido de datos personales

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

establece esa ley, resultan inaplicables para atender la problemática en el ámbito electoral, toda vez que los artículos 67 y 68 refieren, respectivamente, a provocar la vulneración de la seguridad de las bases de datos con ánimo de lucro, a cargo de quien esté autorizado para tratar datos personales, y al tratamiento con fines de lucro de datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

V. La afiliación indebida de un ciudadano a un partido político

Desde un punto de vista histórico y evolutivo, los partidos políticos han afrontado diversas vicisitudes que les han puesto en constante prueba, entre otras: alta competencia en el sistema de partidos, escisiones internas producto del debilitamiento de las identidades partidistas, la necesidad de ampliar o modernizar sus plataformas políticas, la legitimación de su representatividad; y desde luego, la permanente búsqueda de la confianza ciudadana respecto de su actuar.

Concebidos como organizaciones ciudadanas por medio de las cuales se posibilita el acceso al ejercicio del poder público, los partidos políticos son entidades del mayor interés para promover la participación del pueblo en la vida democrática.

En el contexto de la democracia tienen un rol trascendental, puesto que su labor no se limita a las acciones inmanentes a la competencia electoral, la postulación de candidatas y candidatos a cargos de elección popular, la promoción del voto y alentar la participación ciudadana en los comicios; como organizaciones que se diferencian nítidamente de otras facciones, grupos o movimientos con intereses sociales y políticos, su fin último, es la permanente búsqueda por la obtención del poder del Estado, o mantenerlo.

Con posterioridad a la competencia electoral, y en caso de ser recipiendario de la administración directa del poder mediante la legitimación electoral de las mayorías, los partidos políticos constituyen gobierno a través de sus otrora candidatas y candidatos, asumiendo, de conformidad con los plazos constitucionales y legales previamente establecidos, las importantes funciones y responsabilidades del Estado para legislar y ejecutar los mandatos de los electores, pero también, para ser parte del complejo sistema de frenos y contra pesos al ejercicio del poder. Por ello, los partidos

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

políticos son vitales para el desarrollo de la democracia, pues constituyen expresiones de competencia y cultura electoral.

En párrafos antecedentes se señaló que las normas constitucionales reconocen el derecho de los ciudadanos para votar y ser votados para los cargos de elección popular, pero también de forma paralela reconocen libertad a los individuos para que puedan asociarse, organizarse, reunirse y agruparse en torno a intereses comunes, siempre y cuando éstos sean lícitos. Sin embargo, por regla especial, esta libertad puede ser restringida en asuntos de carácter político; es decir, limitarse su práctica, única y exclusivamente, a los individuos que siendo nacionales de un determinado país, y que, teniendo la calidad de ciudadanos, pueden asociarse con fines políticos.

La afiliación a un partido político es un acto libre por medio del cual una persona expresa su voluntad para vincularse jurídica y políticamente con los documentos básicos de un determinado instituto político, lo cual implica un compromiso activo con la ideología partidaria, la declaración de principios, el programa de acción, los estatutos, el código de ética partidista y la plataforma electoral, y a la vez constriñe al cumplimiento de las resoluciones y determinaciones de los distintos órganos directivos, deliberativos, ejecutivos, territoriales y jurisdiccionales, asambleas y consejos de cada partido.

Puede suceder que un partido político afilie indebidamente a un ciudadano como miembro o militante sin que haya mediado su consentimiento, lo cual resulta en un atentado a la libertad de asociación en materia política.

Es importante mencionar que a través de la tesis VIII/2005, emitida con motivo de la resolución del expediente SUP-JDC-803/2002, el TEPJF ha sostenido que, desde la perspectiva de control constitucional y legal de los estatutos de los partidos políticos, debe armonizarse el derecho de asociación de los ciudadanos y la libertad de autoorganización de los institutos políticos, puesto que esta última, si bien es amplia, lo cierto es que se encuentra sujeta a determinados límites, entre ellos, la voluntad de los ciudadanos para afiliarse; de ahí que esta última genere la vinculación entre ciudadano y partido político.

La afiliación indebida a un partido político constituye el uso no autorizado de datos y documentos personales de los ciudadanos. Ante el supuesto de que ello ocurra, los ciudadanos tienen a su alcance mecanismos administrativos y jurídicos de tutela de su fundamental derecho a la libre asociación y pertenencia o no a un partido político.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

A guisa de ejemplo, se erige el particular caso identificado a través de la resolución del expediente SUP-RAP-139/2018, en el cual el TEPJF confirmó el Acuerdo INE/CG445/2018 emitido por el Consejo General del INE, el cual se inició con motivo del procedimiento sancionador ordinario UT/SCG/Q/EGLR/CG/53/2017. En dichos documentos, se evidenció que once ciudadanos fueron afiliados a un partido político nacional en contra de su voluntad, pues el instituto político no acreditó fehacientemente que así hubiese sido.

Aquí es importante destacar que, según el criterio de la Sala Superior del TEPJF, la vía planteada por los quejosos, además de ser idónea, sentó tres criterios trascendentales: 1. Los ciudadanos no tienen la obligación de solicitar su baja del padrón de afiliados de un partido político, cuando no ha sido su voluntad afiliarse; 2. Los ciudadanos no tienen la obligación de agotar previamente las instancias internas establecidas en los estatutos del partido político correspondiente, y 3. Los partidos políticos incurren en infracciones a la normativa electoral y en responsabilidades administrativas con motivo de su negligente actuar, al afiliar indebidamente a un ciudadano.

De lo anterior se colige que los partidos políticos se encuentran obligados a observar y cumplir con el régimen legal de protección de datos personales, cuestión que es trascendental tanto para la afiliación de sus militantes, como para el ejercicio de los derechos político-electorales de los ciudadanos. En este sentido, sea que cuenten con registro nacional o local, de acuerdo con la situación jurídica concreta respecto del tratamiento de datos personales, los partidos políticos deben aplicar una diversidad de normativas en la materia.

Al respecto, la LGPDPPSO resulta aplicable para el tratamiento de la información personal que es proporcionada por aquellas personas que de forma libre y voluntaria deciden afiliarse al instituto político que resulte afín a su ideología, opiniones y/o convicciones. Los partidos políticos deben ser extremadamente cuidadosos para evitar la afiliación indebida de un ciudadano a su padrón de militantes, pues asistirá a éste el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento, o bien, la tramitación de un juicio para la protección de los derechos político-electorales del ciudadano, ya que tal información se circunscribe a la esfera íntima de las personas, es decir, se trata de datos sensibles que requieren de un tratamiento especial a través de la implementación de medidas de seguridad, administrativas, físicas y técnicas que aseguren su confidencialidad bajo estándares superiores, pues en caso de que se incumpla ésta u otras obligaciones respecto del tratamiento de datos perso-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

nales, se fincarán las responsabilidades y se aplicarán las sanciones correspondientes, debiendo ser la autoridad electoral competente la encargada de llevar a cabo la investigación y, en su caso, sanción de las infracciones en que incurra un partido político.

Igualmente, los partidos políticos deben ser también extremadamente cautos y diligentes, en términos de la legislación electoral, frente al tratamiento de las bases de datos relativas al RFE, PE o LNE, con motivo del ejercicio de sus funciones de representación política ante los órganos electorales competentes.

Así, por ejemplo, los representantes de los partidos políticos al estar autorizados para acceder, consultar, revisar o manipular los archivos contenidos en dichas bases, de forma ilícita pueden comercializar, suministrar o transmitir los archivos o las bases de datos, generando con ello no sólo la exposición de la información de las personas que se encuentran inscritas en los registros, padrones o listados; a la vez, pueden desplegar un actuar ilícito que atente en contra del ejercicio de los derechos político-electorales de los ciudadanos, así como incurrir en responsabilidades en los ámbitos electoral, penal y/o civil.

VI. La dispersión ilegal del padrón electoral

Bajo la expresión "dispersión ilícita" enmarcamos determinadas conductas antijurídicas desplegadas por personas que, debido a sus funciones de servicio público o de representación política ante un órgano electoral, se encuentran autorizados para acceder, consultar, revisar o manipular los archivos que contienen las bases de datos relativas al RFE, PE o LNE.

Este particular ámbito de colisión en el tratamiento de los datos personales de los ciudadanos tiene verificativo cuando se poseen, adquieren, comercializan, suministran o transmiten ilícitamente los archivos o las bases de datos, generándose con ello la exposición de la información de las personas que se encuentran inscritas en los registros, padrones o listados.

Estas conductas no se limitan a la materia electoral, pues en el ejercicio de sus atribuciones, las dependencias gubernamentales diseñan y mantienen en operación cotidiana una diversidad de bases de datos, *v. gr.* los padrones de beneficiarios de programas sociales, asistenciales, de salud; las cuales, *per se*, constituyen una importante fuente de información que eventualmente podría ser utilizada con fines distintos a los de su legal y legítimo tratamiento.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

La historia electoral de México registra diversas ocasiones en las cuales el PE fue objeto de exposición o uso ilícito, todas ellas de amplio conocimiento de las autoridades administrativas y jurisdiccionales en materia electoral.

Un primer pasaje tuvo verificativo entre 2002 y 2003, cuando el extinto Instituto Federal Electoral (IFE) reconoció que una empresa de nacionalidad mexicana vendió por doscientos cincuenta mil dólares el PE a la estadounidense ChoicePoint, hoy LexisNexis® Risk Solutions.

El entonces consejero presidente del IFE, José Woldenberg, confirmó que la base de datos contenía la información personal de cincuenta y ocho millones de mexicanos inscritos en todo el país, entre ella, fecha de nacimiento, sexo, apellido paterno y materno, nombre, dirección, estado, municipio, localidad y registro federal de contribuyentes; sin embargo, precisó que no contenía fotografías, huellas dactilares, firmas, clave de elector, folio, estado, distrito, número de credencial y ninguna información de tipo electoral.

Un segundo evento se verificó entre 2005 y 2006. En ese entonces la Coalición por el Bien de Todos, integrada por los partidos políticos de la Revolución Democrática, Convergencia y del Trabajo, denunciaron ante el IFE al Partido Acción Nacional, porque durante la etapa de campaña del proceso electoral 2005-2006, promovió la construcción de redes ciudadanas de apoyo a su candidato presidencial mediante un procedimiento de registro de simpatizantes a través de su sitio de internet. Ahí, los ciudadanos podían aportar sus datos para inscribirse en las redes de apoyo, pero el sistema electrónico no permitía su registro si los datos que proporcionaban no coincidían con el nombre y fecha de nacimiento asentados en su credencial para votar con fotografía.

Sobre estos hechos, el Consejo General del IFE determinó sancionar al Partido Acción Nacional. Inconforme con esa determinación, la dirigencia nacional de ese instituto político la apeló ante el TEPJF, quien correspondientemente integró los expedientes SUP-RAP-76/2007 y SUP-RAP-81/2007, en donde la Sala Superior, además de ordenar al IFE impusiera al Partido Acción Nacional una multa ejemplar por reincidir en la violación a la confidencialidad de los datos contenidos en una LNE, se pronunció sobre la utilización indebida del PE y, estableció un criterio para determinar en qué casos es posible poner en riesgo la confidencialidad de los datos que lo integran.

Finalmente, no debe pasar inadvertido que durante 2016, Adam Tanner, becario de Investigación del Instituto para Ciencias Sociales Cuantitativas de la Universidad de Harvard, y Chris Vickery, director de Cyber

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Risk Research, hicieron del conocimiento del INE el alojamiento en uno de los servidores de internet de Amazon Web Services, de una base de datos que contenía los nombres y domicilios de más de noventa y tres millones de votantes de México.

Por el volumen de registros expuestos, y el daño a la credibilidad de la autoridad administrativa electoral, así como de los resultados del proceso electoral federal 2014-2015, el INE se dio a la tarea de aplicar los protocolos que permitieran obtener y resguardar la información que sirviera para conocer la veracidad de los hechos. En este sentido, a través de las áreas especializadas, aplicó el denominado "Protocolo para Obtener la Copia del Disco de ADN", el cual es un procedimiento de recuperación de información que consiste en obtener abreviaturas y/o símbolos incorporados en los registros de los ciudadanos de la LNE, ello mediante un mecanismo sistematizado de marcado digital individualizado y diferenciado para cada uno de los archivos, logrando así una plena identificación y correspondencia de cada representante de partido político al que le haya sido entregado, es decir, la autoridad electoral no entregó el mismo archivo a los representantes de todos y cada uno de los partidos políticos acreditados, sino que a cada uno le fue entregado un archivo, que si bien contenía esencialmente la misma información del PE, lo cierto es que, en su origen fue diferenciado a través de la inserción de un código específico, lo cual le convirtió en un archivo único, y por lo tanto, capaz de ser diferenciado a los demás generados y entregados.

Tanto en la investigación administrativa, como en la sustanciación del recurso de apelación SUP-RAP-96/2018 y acumulados, las autoridades electorales concluyeron que el archivo alojado en internet y el entregado al partido político Movimiento Ciudadano, correspondían a la LNE entregada para su revisión a los partidos políticos acreditados ante las comisiones de vigilancia.

A propósito del recurso de apelación, el TEPJF además de corroborar la ilicitud de la conducta frente a la legislación electoral, con el propósito de generar un efecto inhibidor, ordenó sancionar tanto al partido político como a las personas físicas involucradas.

Sin embargo, y por así corresponder estrictamente a sus competencias, se limitó a pronunciarse respecto a la juridicidad administrativa de los hechos, obviando en consecuencia referirse a lo previsto en la fracción II del artículo 13 de la LGMDE, en la que se establece la imposición de 70 a 200 días multa y prisión de tres a siete años, a quien altere, falsifique, destruya, posea, use, adquiera, comercialice, suministre o transmita de manera ilegal, archivos o datos de cualquier naturaleza, relativos al RFE, PE o LNE;

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

punibilidad que se incrementará hasta un tercio más, en caso de que se trate de servidor público, funcionario partidista, precandidato o candidato el que intervenga en la comisión de las conductas prohibidas.

VII. Conclusiones

La protección de datos personales de los ciudadanos en el ámbito político-electoral mexicano, además de encontrarse regulada en diversas disposiciones legales, y ejercerse a través de distintas vías administrativas y jurisdiccionales, depende en gran medida de la relación jurídica concreta del ciudadano, es decir, está condicionada a determinarse si se trata de una actividad de carácter político, electoral o preelectoral, pues las normas jurídicas electorales y las relativas a la protección de datos personales establecen procedimientos diferenciados que podrán ser tramitados ante las autoridades electorales, los partidos políticos, los ciudadanos que aspiren a un cargo de elección popular por la vía independiente, o ante la jurisdicción constitucional de la libertad político-electoral.

Consideramos que, para minimizar el riesgo de violación a la confidencialidad de los datos personales de carácter político-electoral, deben reforzarse los controles preventivos de vigilancia y cumplimiento que realizan las autoridades electorales respecto de las obligaciones y responsabilidades de los distintos actores políticos; y a la par, inhibir la reiteración de conductas ilícitas mediante la imposición de sanciones estrictas y ejemplares.

Debe promoverse, desde el punto de vista técnico-jurídico, la armonización de la legislación y la jurisprudencia relativa a la protección de datos personales en posesión de autoridades electorales, partidos políticos y demás participantes en los procesos político-electorales, ya que la existencia de diferentes grados de protección jurídica genera colisiones normativas que, además de estimular malas prácticas electorales, aumentan la desconfianza ciudadana en el actuar de todos los actores políticos, lo cual incide negativamente en la salvaguarda de la intimidad político-electoral y en la vigencia de los principios de certeza, legalidad y objetividad que rigen a la organización, desarrollo y vigilancia de los procesos electorales.

VIII. Bibliografía

Barriuso Ruiz, Carlos, 1996, *Interacción del derecho y la informática*, Madrid, Dykinson.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Corte Interamericana de Derechos Humanos, 2008, *Caso Castañeda Gutman vs. Estados Unidos Mexicanos*, Sentencia de 6 de agosto de 2008.

Duverger, Maurice, 1970, *Instituciones políticas y derecho constitucional*, Barcelona, Ariel.

Ekmekdjian, Miguel Ángel y Pizzolo, Calogero, 1996, *Hábeas data: el derecho a la intimidad frente a la revolución informática*, Buenos Aires, Depalma.

Instituto Electoral del Estado de México (IEEM), 2019, *Estudio sobre la calidad de la ciudadanía en el Estado de México*, disponible en *http://ieem.org.mx/cefode/descargas/investigaciones/Estudiociudadania.pdf*.

Instituto Nacional de Estadística y Geografía (INEGI), 2017, Encuesta Nacional de Calidad e Impacto Gubernamental, disponible en *https://www.inegi.org.mx/programas/encig/2017/*.

Instituto Nacional Electoral, Acuerdo INE/CG295/2018, disponible en *https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/95581/CGesp201803-29-ap-2-9.pdf*.

Instituto Nacional Electoral, Acuerdo INE/CG426/2017, disponible en *https://repositoriodocumental.ine.mx/xmlui/bitstream/handle/123456789/93572/CGex201709-08-ap-11.pdf?sequence=1&isAllowed =y*.

Instituto Nacional Electoral, Acuerdo INE/CG387/2017, disponible en *https://portal.ine.mx/wp-content/uploads/2017/09/CGex201708-28-ap-12.pdf*.

Instituto Nacional Electoral (INE), 2015, Informe País sobre la Calidad de la Ciudadanía en México, disponible en *https://portalanterior.ine.mx/archivos2/portal/DECEYEC/EducacionCivica/informePais/*.

Instituto Nacional Electoral, Convocatoria a las Ciudadanas y los Ciudadanos con Interés en Postularse como Candidatas o Candidatos Independientes a la Presidencia de la República, Senadurías o Diputaciones Federales por el Principio de Mayoría Relativa, 2017, disponible en *https://www.ine.mx/wp-content/uploads/2017/09/DEPPP-CI-Convocatoria.pdf*.

Kelsen, Hans, 1993, *Teoría pura del derecho*, México, Porrúa.

Lucas Murillo, Pablo, 1990, *El derecho a la autodeterminación informativa*, Madrid, Tecnos.

Méndez de Hoyos, Irma, 2017, "La manipulación del marco legal de las elecciones en América Latina entre 2000 y 2012: una aproximación metodológica". *Foro Internacional*, vol. 57, núm. 3, disponible en *https://dx.doi.org/10.24201/fi.v52i3.2451*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Pérez Luño, Antonio-Enrique, 1996, *Manual de informática y derecho*, Barcelona, Ariel.

Pérez Luño, Antonio-Enrique, 1989, "Los derechos humanos en la sociedad tecnológica", en Losano, Mario G. *et al*., *Libertad informática y leyes de protección de datos personales*, Madrid, Centro de Estudios Constitucionales.

Pierini, Alicia *et al*., 1999, *Habeas Data*, Buenos Aires, Universidad.

Sieyès, Emmanuel J., 1989, *¿Qué es el Tercer Estado?*, México, UNAM.

Villanueva, Ernesto y Díaz, Vanessa, 2015, *Derecho de las nuevas tecnologías*, México, Oxford.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

EL ENFOQUE DE CAPACIDADES EN LA PROMOCIÓN DEL DERECHO A LA INFORMACIÓN EN COMUNIDADES EN VULNERABILIDAD

THE CAPABILITIES APPROACH FOR PROMOTING THE RIGHT TO INFORMATION IN VULNERABLE COMMUNITIES

Víctor Alejandro VILLEGAS CORONA*

RESUMEN. El derecho a la información es un derecho humano de utilidad para la exigencia de otros derechos y la participación en el espacio público; sin embargo, la información pública no está al alcance de todas las personas de forma equitativa debido a barreras como la digital, la escolaridad, la alfabetización, la pobreza económica, la etnia, el género, entre otras. Mientras que las políticas de promoción del derecho a la información se han basado en difusión en medios masivos y proyectos con enfoque de "formación de usuario", que no necesariamente consideran el desarrollo de capacidades en las personas y la reducción de barreras para el acceso y el uso de información pública de sectores en vulnerabilidad. Este artículo propone el uso del enfoque de capacidades en las políticas de promoción del derecho a la información, para lograr que las personas puedan usar información pública como herramienta indispensable de la capacidad de control sobre su entorno político. Para ello, se desarrolla un marco analítico de capacidades de acceso y uso de información pública y se aplica en un estudio de caso del programa "Transparencia proactiva" de Artículo 19 México y Centroamérica, que promueve el derecho a la información en comunidades rurales

* Licenciado en Ciencias políticas y administración pública, y maestro en Gobierno y asuntos públicos por la Universidad Nacional Autónoma de México; miembro de Arkemetría Social, A. C. *victorvillegas@politicas.unam.mx*.

Fecha de recepción: 11 de julio de 2019.
Fecha de dictamen: 22 de noviembre de 2019.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

y mayoritariamente indígenas en Chiapas, México, con la finalidad de identificar estrategias orientadas al desarrollo de capacidades para el acceso y uso de información pública. A partir de ello, se ofrecen algunas recomendaciones desde el enfoque de capacidades para mejorar las políticas públicas de promoción del derecho a la información en personas en vulnerabilidad.

PALABRAS CLAVE. Derecho a la información, enfoque de capacidades, desarrollo humano, transparencia proactiva, poblaciones en vulnerabilidad, pueblos indígenas.

*ABSTRACT. The right to information is a useful human right for the demand of other rights and for participation in public space; however, public information is not available equally for all people due to barriers as digital, literacy, schooling, underprivileged economic situation, gender, language and/or ethnicity. While right to information promotion policies have been based on dissemination on mass media and projects with a "user training" approach, which do not necessarily consider the development of capabilities of people nor reduce barriers to access and use of public information, especially in vulnerable sectors. The aim of this article is to propose the use of the capabilities approach in public policies to promote the right to information, so that people can use public information as an indispensable tool for the capability to control their political environment. To do this, an analytical model of capabilities for access and use of public information is developed and applied in a case study of "*Transparencia proactiva*", a program by Article 19 Mexico and Central America which promotes right to information in rural and mostly indigenous communities in the northern jungle of Chiapas, Mexico, in order to identify strategies focused on developing capabilities for access and use of public information. Based on this, some public policy recommendations are offered, from the capabilities approach to improve public policies to promote right to information in vulnerable people.*

KEYWORDS. Right to information, capabilities approach, human development, proactive transparency, vulnerable people, indigenous people.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

I. Introducción

El derecho a la información pública (DI) en México no es accesible ni de utilidad para las personas en situación de vulnerabilidad. Existen evidencias empíricas que indican que las desventajas por pobreza, grado de estudios, conectividad y pertenencia a un grupo indígena impactan negativamente en el ejercicio del derecho (Zermeño, 2010). No obstante, las acciones de promoción del derecho están basadas en la difusión masiva y programas de socialización con un enfoque de formación de usuarios del derecho, con lo que no se garantiza el desarrollo de conocimientos y habilidades requeridos para ejercer el DI.

El problema de investigación es que actualmente las leyes y programas mexicanos no conciben al ejercicio del derecho a la información pública como un proceso amplio que requiere considerar los contextos de las personas, sus conocimientos y habilidades para acceder y usar información pública en el logro de objetivos. La pregunta central de investigación es ¿de qué manera se puede incorporar el enfoque de capacidades en las estrategias para promover el acceso y uso de información pública por parte de personas en situación de vulnerabilidad?

El argumento central es que el ejercicio de DI forma parte fundamental de la capacidad de control sobre el propio entorno político (Nussbaum, 2012), en tanto es indispensable para la vigilancia de los gobiernos y la participación en los asuntos públicos. Es por ello que las políticas públicas de promoción del derecho deben desarrollar estrategias centradas en las personas en vulnerabilidad y sus contextos, y fortalecer habilidades y capacidades para obtener y usar información pública en el marco de sus libertades.

Con la base teórica del desarrollo de capacidades (Sen 2000, 2005; Nussbaum 2000, 2012) se revisan aportaciones que proponen concebir el acceso a la información como una cuestión de capacidades y habilidades, y se construye un modelo analítico basado en cinco niveles de acceso a la información pública. Este marco analítico fue de utilidad para el estudio de caso de un programa considerado emblemático por el desarrollo de capacidades para ejercer el DI en comunidades indígenas.

Cabe mencionar que esta investigación tiene un carácter exploratorio, pretende establecer un diálogo entre el enfoque de capacidades y los estudios académicos del acceso a la información, con la finalidad de proponer mejoras a las políticas públicas para que atienda las barreras que dificultan

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

e impiden el pleno acceso y uso de la información pública a las personas en situación de vulnerabilidad.

Ahora bien, la investigación pone especial atención en el acceso a información pública en el ámbito digital debido a que las legislaciones en México obligan a todos los organismos públicos a responder solicitudes y difundir información preponderantemente de forma electrónica, vía Plataforma Nacional de Transparencia (PNT). No obstante, se reconoce que la información pública dirigida a personas en vulnerabilidad debe ser accesible por otros medios más allá de los digitales.

En el apartado II, se describen las políticas de promoción del DI en México, con especial atención por mostrar las limitaciones de los enfoques de promoción masiva y formación de usuarios. En la tercera parte, se discute la vinculación del DI con el enfoque de capacidades, argumentando por qué es un derecho indispensable para el acceso a otros derechos, la participación en asuntos públicos y el control del entorno político de las personas.

Posteriormente, en el cuarto apartado, se discuten distintas aportaciones teóricas y empíricas que han estudiado el acceso a la información de las personas como una cuestión de capacidades y habilidades digitales, intelectuales y cívicas, ámbitos que forman parte del alfabetismo informacional (Sturges, 2010). Con base en esto, se construye un marco analítico de utilidad para estudiar estrategias enfocadas en fomentar el DI en comunidades en vulnerabilidad.

En el parte quinta, se presenta la estrategia metodológica utilizada, incluyendo la justificación de la selección del estudio de caso y las fuentes de investigación empleadas. En el apartado VI se presentan los resultados del estudio de caso del programa "Transparencia proactiva" de Artículo 19 México y Centroamérica, que se enfoca en desarrollar capacidades en mujeres y comunidades indígenas de Chiapas, México, para el uso de información pública en la exigencia de otros derechos humanos (Artículo 19, 2017).

Con base en la discusión teórica y los hallazgos del estudio de caso, en la última parte (VII) se realizan algunas propuestas para mejorar la política pública de socialización del DI en México, para lograr que las personas en situación de vulnerabilidad desarrollen las capacidades y habilidades necesarias para el acceso y uso de información pública en el logro de objetivos personales o comunitarios, como parte de su capacidad de control de su entorno político.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

II. Panorama de las políticas de promoción del derecho a la información pública en México

Desde 2002, México cuenta con una ley de acceso a información pública, que se ha mantenido como un referente internacional (Access Info Europe and the Centre for Law and Democracy, 2016). El marco normativo ha incluido estándares internacionales que consideran la educación al público sobre el derecho con énfasis en estrategias alternativas acordes con los niveles de alfabetización (Artículo 19, 1999).

En este sentido, las actividades de promoción del DI por parte del organismo garante federal, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI —antes IFAI—), se han orientado a la difusión propagandística por medios de comunicación masiva que informan a las personas sobre su derecho. Al respecto, de 2003 a 2017 el Instituto gastó en promedio alrededor de cuatro millones de pesos anuales en difusión de anuncios promocionales a través de radio, televisión y espacios publicitarios.[1]

Por otro lado, también se han desarrollado programas de intervención directa con poblaciones objetivo. Entre 2005 y 2007 se implementó el Proyecto Comunidades: programa piloto desarrollado por el IFAI en colaboración con organizaciones de la sociedad civil, orientado a promover el derecho entre personas de grupos en situación de vulnerabilidad, con el fin de identificar las mejores metodologías y estrategias para lograr la apropiación del DI.

Con la evaluación realizada a este programa, se evidenció empíricamente que los bajos niveles de escolaridad o la pertenencia a un grupo indígena complican el ejercicio autónomo del derecho posterior a las intervenciones (Zermeño, 2010). Por lo cual es necesario construir estrategias específicas para lograr disminuir los efectos de las barreras causadas por elementos como la falta de conectividad y el analfabetismo.

En 2008, el IFAI decidió no continuar con el Proyecto Comunidades, y no existieron iniciativas parecidas hasta después de 2015, con la publicación de la Ley General de Transparencia y Acceso a la Información Pública, en cuyo artículo 54 se indica la obligación de los organismos garantes de "desarrollar programas de formación de usuarios de este derecho para incrementar su ejercicio y aprovechamiento, privilegiando a integrantes de sectores vulnerables o marginados de la población".

[1] Respuesta a la solicitud de acceso a la información con folio 0673800231117, realizada al INAI.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

En 2015 se comenzó a desarrollar el Programa de Sensibilización de Derechos (Prosede), con el que cada año se convoca a organizaciones de la sociedad civil a promover los derechos a la información y protección de datos personales en distintas poblaciones objetivo. Es importante mencionar que entre 2016 y 2018, el programa contó con un presupuesto promedio de alrededor de dos millones de pesos anuales, prácticamente la mitad de lo gastado en anuncios cada año,[2] lo que muestra la preponderancia de la difusión masiva frente a la búsqueda de metodologías exitosas de intervención directa en la población.

Por otro lado, los proyectos financiados por el programa Prosede cuentan con un tiempo promedio de implementación de alrededor de cuatro meses al año, y solamente unos cuantos proyectos han logrado obtener recursos financieros para dar continuidad a sus actividades por más de un año. Esta es una limitación en el diseño del programa, pues como Zermeño (2010) demostró, los periodos cortos de capacitación y la ausencia de continuidad tienen impactos negativos en el desarrollo de conocimientos y habilidades requeridas para ejercer el DI.

Ahora bien, en 2017 se publicó el Programa Nacional de Transparencia y Acceso a la Información 2017-2021, que establece una relación entre la promoción y socialización del DI como herramienta para el acceso a salud, educación y servicios. Con base en este programa, durante 2018 se construyó el Plan Nacional de Socialización del Derecho de Acceso a la Información (PlanDAI), el cual busca homologar las acciones de los organismos garantes para la promoción del derecho y generar estrategias focalizadas en el aprovechamiento de la información pública (INAI, 2018).

Es necesario hacer notar que el PlanDAI está primordialmente orientado a la formación "usuarios" del derecho, es decir de los procesos y plataformas disponibles para ejercerlo. La definición del problema reconoce causas como la complejidad de los procesos para ejercer el derecho y el incumplimiento de los servidores públicos; también se identifican los bajos niveles de conocimiento y la percepción de utilidad del derecho (INAI, 2018: 8).

Con este diagnóstico, la propuesta busca incidir en la segunda vertiente de causas de la problemática, el conocimiento y la percepción sobre el derecho; es decir, se busca modificar la opinión que tienen las personas sobre el DI como un derecho útil o aprovechable, con acciones como la difusión de videos con casos éxito, la entrega de reconocimientos y otras

[2] Solicitud de acceso a la información con folio 0673800231117, dirigida al INAI.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

estrategias de promoción masiva que se han usado antes y cuyos impactos no son demostrables.

Si bien la propuesta maneja la idea de aprovechamiento del derecho, que incluye la utilización de información para fines determinados, también reconoce que "para concretar el aprovechamiento del DAI, necesariamente deberán existir o generarse las capacidades suficientes en los usuarios" (INAI, 2018: 4). Sin embargo, no se identifica qué tipos de capacidades se deberán desarrollar y los objetivos más allá de la formación de usuarios de las plataformas electrónicas de información; esto representa una limitante importante en el planteamiento de política.

Un elemento destacado del Plan es que busca continuar con los esfuerzos de establecer alianzas con organizaciones de la sociedad civil con experiencia en campo, y de formar personas facilitadoras para promover el derecho, que repliquen las capacitaciones con otros grupos de la población. En 2018 se desarrollaron dos ejercicios piloto a nivel local en Oaxaca y Nayarit, con talleres enfocados en beneficiarios de programas sociales y pueblos indígenas. Con esto se hicieron recomendaciones como la participación de traductores de las lenguas indígenas y la adaptación de las actividades a los contextos y perfiles de participantes.

Como se observa, las acciones de promoción del DI en México han privilegiado un enfoque de difusión en medios masivos, los cuales resultan limitados en la transmisión de conocimientos y habilidades para el ejercicio del DI. Por el contrario, los programas de intervención en grupos definidos de la población cuentan con potencial para generar impactos medibles en las habilidades de las personas y comunidades atendidas, así como la posibilidad de sistematización y contrastación empírica de metodologías en distintos contextos.

A continuación, se realiza una discusión sobre el enfoque teórico de capacidades y se argumenta que podría ser de utilidad para modificar las políticas de promoción del DI y lograr intervenciones centradas en las personas y sus contextos.

III. El derecho a la información pública como una cuestión de capacidades, discusión teórico-conceptual

Los derechos a la información se desarrollaron con la consolidación de la sociedad informacional, en la cual, la economía y las relaciones políticas y sociales están basadas en la producción de información y dispositivos para intercambiarla (Castells, 1997). De acuerdo con Bovens (2002), las condi-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

ciones de esta era histórica requieren el reconocimiento de derechos que garanticen a todas las personas el acceso a información "socialmente relevante", que facilite la toma de decisiones públicas y el monitoreo de los gobiernos.

En este sentido, el reconocimiento del DI también es una cuestión de justicia social, pues en esta era la información juega un papel fundamental en el desarrollo de las personas (Bovens, 2002: 14). La información, como bien público elemental, debe ser garantizada por los gobiernos para posibilitar la participación de las personas en asuntos colectivos (Stiglitz, 1999; 2000); asimismo se ha reconocido que "la falta de información genera asimetrías económico-sociales que ponen en desventaja a ciertos grupos de la población frente a otros" (Luna, 2013: 78).

Debido a la importancia de la información para el desarrollo de las personas y el ejercicio de sus derechos, en la era informacional las garantías de información son equiparables con las garantías de debido proceso en la administración de justicia, "también son consideradas derechos en sí mismos, y requisitos de la existencia de otros derechos. De modo que la información tiene, además de un valor propio, un valor instrumental, [para el] ejercicio de otros derechos y [el] funcionamiento institucional de contralor de los poderes públicos" (Abramovich y Courtis, 2000: 1).

Aún con la importancia capital del DI, algunos estudios consideran que las leyes y políticas en la materia se han centrado en ajustes superficiales y modificaciones discursivas para la legitimación de los gobiernos, como una cuestión de higiene pública (Bovens, 2002). También se sostiene que las leyes consideran a las personas como "usuarias" del derecho y no necesariamente como ciudadanas, que acceden a información pública como una herramienta para lograr rendición de cuentas y participación ciudadana (Sandoval, 2013).

En esta investigación se plantea la problemática del acceso a información pública como una cuestión de justicia distributiva de bienes públicos. Con el marco conceptual de la sociedad informacional, la información es un bien público fundamental que, debido a barreras como la conectividad, la etnia y el género, no está al alcance de todas las personas de forma equitativa. Es por ello que se propone discutir el enfoque de capacidades para el desarrollo humano como una herramienta útil para considerar los contextos y barreras de las personas en situación de vulnerabilidad.

El enfoque de capacidades es una corriente teórica con una amplia justificación filosófica inaugurada por Amartya Sen (2000), economista que desarrolló una sólida crítica a los enfoques dominantes que equiparaban el desarrollo con el crecimiento económico. También se ofrecieron

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

elementos alternativos a las mediciones tradicionales del bienestar de las personas en función con los bienes económicos y materiales con los que cuenta o a los que puede acceder (Sen, 2016; Deneulin y Stewart, 2002).

La alternativa teórica y empírica iniciada por Sen, propuso poner en el centro de análisis a las personas, sus contextos, libertades y oportunidades, como una alternativa para conceptualizar y medir el desarrollo y el bienestar (Sen, 2000; Robeyns, 2005; Urquijo, 2014), y se caracteriza porque "pone la agencia humana (en lugar de la agencia de organizaciones como mercados o gobiernos) en el centro del escenario" (Dreze y Sen, 2002: 6). Bajo este enfoque, se conceptualiza y valora la desigualdad, la calidad de vida y el bienestar de las personas como un asunto del ejercicio de sus libertades y su autorrealización.

El enfoque de capacidades se interesa por las cosas que las personas pueden hacer y ser. Es decir, por un lado, los funcionamientos, que se refiere a las actividades que puede hacer; y por el otro, las capacidades, que consideran lo que la persona puede lograr cuando decide realizar esas acciones como parte de sus libertades (Sen, 2000, 2005). Dicho de otra forma, el enfoque analiza las libertades con que cuentan las personas para elegir entre las oportunidades a su alcance, las más idóneas para alcanzar las cosas que valora en su vida y sus propias ideas de lo que significa el bienestar.

Distintos estudios se han centrado en la operacionalización del concepto de capacidades, que permitan entender el enfoque y aplicarlo en la práctica; en este sentido, resulta necesario hacer énfasis en la distinción entre bienes, funcionamientos y su relación con las capacidades (Fukuda-Parr, 2003; Saith, 2001) Un ejemplo que puede ilustrar claramente esta distinción es pensar que, el valor de un bien, como una bicicleta, no se basa únicamente en los materiales de los que está hecha, sino en su utilidad para la movilidad. El desarrollo de capacidades se observaría en la medida de que la persona elige utilizar un bien (montar en bicicleta) para ejercer el funcionamiento de movilidad, como parte de sus alternativas para alcanzar su idea particular de bienestar (usarla como medio de transporte o para ejercitarse) (Robeyns, 2005: 98-99).

Continuando con la metáfora, algunas personas, como las que cuentan con alguna discapacidad, no podrán utilizar los bienes en igualdad de condiciones, por lo que se debe considerar las limitaciones y contextos de las personas (Urquijo, 2014; Fukuda-Parr, 2003; Saith, 2001). Además, el enfoque otorga especial importancia a las oportunidades, o lo que los gobiernos y otras instituciones hacen para garantizar las condiciones adecuadas para el ejercicio de los derechos y las libertades; incluso se afirma

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

que no se puede analizar el desempeño individual sin considerar que las opciones al alcance de las personas y las oportunidades para mejorar la calidad de sus vidas dependen de las condiciones sociales y la acción del estado (Dreze & Sen, 2002: 6).

Desde 1990, el Programa de Naciones Unidas para el Desarrollo adoptó el enfoque de capacidades de Sen para la construcción del Índice de Desarrollo Humano, con el cual el organismo pasó de tomar en cuenta únicamente el crecimiento económico de los países, a considerar que "el objetivo básico del desarrollo es aumentar las libertades humanas en un proceso que puede expandir las capacidades personales toda vez que amplía las alternativas disponibles para que la gente viva una vida plena y creativa" (PNUD, 2004: 127; 2009)

Ahora bien, el enfoque de capacidades se enriqueció de forma considerable con las aportaciones de Martha Nussbaum (2000, 2003, 2004), quien, desde una perspectiva narrativa profundizó con casos prácticos sobre la vida de las personas y las barreras a las que se enfrentan para ejercer sus derechos y sus libertades. La autora puso especial atención en la delimitación de la idea de capacidades en el marco de una teoría más amplia de justicia social, a partir de la cual, las personas de todo el mundo puedan ejercer sus libertades y procurarse bienestar sin importar su género, cultura o situación económica.

Nussbaum distingue varios niveles en los que se integran las capacidades internas de las personas con los elementos externos que pueden facilitar u obstaculizar la elección de alternativas y el ejercicio de libertades (Nussbaum, 2000). Por otro lado, su propuesta destaca por la discusión sobre las capacidades de razón práctica y afiliación, poniendo atención en la necesidad de articularlas con el desarrollo de pensamiento crítico como un elemento indispensable en la educación de las personas en democracias (Nussbaum, 2011).

Cabe mencionar que la diferencia más notable entre las aportaciones de Sen y Nussbaum es la propuesta de la autora sobre un listado mínimo de capacidades centrales que deberían ser garantizadas universalmente y reconocidas por las constituciones políticas (Nussbaum, 2003; 2012). En este sentido, Sen se ha posicionado en contra de definir una lista definitiva de capacidades mínimas, pues eso limitaría las posibilidades de redefinirla a través de discusiones colectivas y de adaptarla a distintos contextos y objetivos (Sen, 2004).

Ahora bien, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, en la Cumbre Mundial sobre la Sociedad de la Información (2003), estableció una vinculación directa entre el enfoque

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

de capacidades y el marco teórico de la sociedad informacional. Bajo este enfoque, se reconoce la importancia de la educación para lograr oportunidades para el acceso y uso de información en la generación de conocimientos y el desarrollo de las personas (UNESCO, 2003; Ríos, 2017).

Por otro lado, también se han establecido vínculos entre el enfoque y los derechos humanos; de acuerdo con Sen (2004), aunque una persona cuente con un derecho garantizado constitucionalmente, puede que las condiciones contextuales limiten en la práctica que las personas ejerzan su derecho. De manera que, el enfoque de capacidades hace necesario ver más allá de la simple consagración de un derecho, y poner atención en los contextos de las personas para asegurar que efectivamente puedan ejercer esos derechos como medio para desarrollar sus libertades y alcanzar su idea de bienestar.

Desde el enfoque de capacidades, la información es un bien público que no está al alcance de todas las personas en igualdad de condiciones, por lo que es necesario estudiar "desde qué condición personal los sujetos pueden o no apropiarse de esta información, integrándola a sus capacidades, con las cuales construye su realización y su libertad" (Ríos, 2017: 32). En esta investigación se vincula el ejercicio del DI con el concepto empleado por Zermeño (2010: 100), quien propone que la apropiación del derecho se observa "cuando un individuo u organización es capaz de allegarse información pública que puede utilizar con un objetivo determinado".

En este sentido se sugiere que el ejercicio del DI, al igual que otros derechos humanos, pueden ser analizados desde el enfoque de capacidades. La importancia del fomento del DI radica en la posibilidad de que las personas puedan elegir ejercerlo como herramienta para el logro de objetivos personales, o bien, para fines colectivos como la discusión en los asuntos públicos y la exigencia de otros derechos humanos.

En esta investigación se utiliza la perspectiva de Nussbaum (2012), pues se coincide con la necesidad de definir algunas capacidades que deben ser reconocidas y garantizadas por los gobiernos. Además, la perspectiva es útil para la investigación, porque "la noción de capacidades de Nussbaum pone más atención a las habilidades de las personas y los rasgos de personalidad [por lo que] tiene más potencial para entender acciones, intenciones y motivaciones (Robeyns, 2005: 104)".

Se afirma entonces que el ejercicio del DI, y en particular el acceso, procesamiento y uso de la información pública, podría considerarse un funcionamiento; es decir, lo que una persona puede elegir hacer como parte de sus capacidades. En específico se sugiere que la apropiación de información pública resulta fundamental para la capacidad de control del

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

propio entorno político, que significa "poder participar de forma efectiva en las decisiones políticas que gobiernan nuestra vida; tener derecho a la participación política y a la protección de la libertad de expresión y de asociación" (Nussbaum, 2012: 54).

En la siguiente tabla se esquematiza la propuesta de vinculación entre el DI y el enfoque de capacidades, indicando la relación de la información pública como bien, el acceso y uso de información pública en la consecución de objetivos, o la apropiación del DI como funcionamiento, mismo que forma parte de la capacidad de control sobre el entorno político. Se compara con el ejemplo de la bicicleta propuesto por Robeyns (2005) para facilitar su comprensión.

Tabla 1. El derecho a la información pública desde el enfoque de capacidades. Relación entre bien, funcionamiento y capacidad

	Bienes	*Funcionamientos*	*Capacidades*
Ejemplo (Robeyns, 2005: 98-99)	Bicicleta	Montar en bicicleta para la movilidad	Elegir usar la bicicleta para ejercitarse o transportarse y alcanzar idea propia de bienestar
Aplicación en derecho a la información	Información pública	Ejercer el DI, buscar y difundir información pública para el logro de objetivos. Apropiación del derecho (Zermeño, 2010)	Elegir ejercer el DI para el control del propio entorno político (incluye libertad de expresión, asociación y participación política) (Nussbaum, 2012: 54)

Fuente: elaboración propia con base en (Robeyns, 2005; Zermeño, 2010; Nussbaum 2012).

El enfoque de capacidades puede ser de utilidad para promover el DI como una cuestión de justicia social, que debe considerar los contextos y

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

las barreras que enfrentan las personas en vulnerabilidad, en el ejercicio de sus derechos para alcanzar su propia idea de bienestar. Enseguida, se revisan aportaciones teóricas y empíricas que han estudiado el acceso a información como una cuestión de capacidades y habilidades.

IV. Categorías de análisis: capacidades y habilidades para el acceso a la información pública[3]

Investigaciones que conciben el acceso a la información de las personas como una cuestión de capacidades y habilidades, han sido desarrolladas desde hace varias décadas por las teorías de pobreza informacional. Surgidos en los años setenta, estos estudios evidenciaron conexiones entre la pobreza económica y el uso de información en la resolución de problemas, así como comportamientos y actitudes que pueden limitar el acceso a la información (Childers y Post, 1975).

Dentro de esta corriente teórica, las aportaciones demostraron que además de la disponibilidad de los medios digitales y las habilidades para manejarlos (acceso físico), las personas requieren capacidades intelectuales para valorar la utilidad de la información, procesarla y comprenderla (acceso intelectual). También se propuso que las personas pertenecen a "pequeños mundos informacionales" en sus comunidades, que comparten actitudes y creencias que pueden propiciar el acceso o la censura de la información (acceso social) (Burnett, 2008; Chatman, 2000; Luna, 2012).

Entre las barreras para el acceso a la información, identificadas en las categorías de los estudios de pobreza informacional, se encuentran las barreras digitales; asimismo, las limitaciones intelectuales, como bajas capacidades de asimilación y/o desciframiento de la información, que impidan procesarla y utilizarla. Además, se sugiere que las personas pueden contar con barreras de carácter social, como prejuicios e ideas compartidas en su comunidad que determinen su rechazo a la información (Burnett, 2008).

Estas aportaciones teóricas están relacionadas directamente con las perspectivas de alfabetismo digital, que se preocupan por la exclusión de personas de los medios donde se distribuye la información (Eshet-Alkalai, 2004); así como los estudios de alfabetismo informacional, que consideran las habilidades para comprender y procesar información (Doyle, 1994).

[3] En la construcción de categorías analíticas, se utiliza el binomio "capacidades y habilidades", para distinguirlas claramente de la capacidad (*capability*) de control del entorno político.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

De acuerdo con Bawden (2001), en la era informacional los alfabetismos digitales e informacionales están íntimamente relacionados entre sí. La perspectiva teórica de pobreza informacional considera ambos tipos de alfabetización, su valor agregado es el estudio de las cuestiones sociales y comunitarias, que pueden determinar el acceso (Chatman, 2000).

Ahora bien, dado que este estudio se enfoca en información de carácter público, es necesario prestar atención en las actitudes y barreras con las que cuentan las personas para participar en el espacio público como miembros de comunidades políticas. En este sentido, algunas aportaciones teóricas se han centrado en discutir sobre los conocimientos y capacidades para la participación política con información.

El alfabetismo cívico se refiere al "conocimiento y la capacidad de los ciudadanos para hacer sentido en su mundo político" (Milner, 2002: 2) y considera dos dimensiones medibles del concepto: en primer lugar, la habilidad, entendida como el conocimiento político; y, en segundo lugar, la voluntad, observada como la participación. El concepto engloba las competencias y el conocimiento necesario para que las personas participen como miembros de una comunidad política y asegurar que sus intereses sean tomados en cuenta.

De acuerdo con el autor, un mayor conocimiento sobre los asuntos públicos, aunado a una conciencia como sujetos miembros de una comunidad política por parte de las personas, implica que serán más propensas a involucrarse activamente en el espacio cívico; es decir, a mayor conocimiento político se tendrá una mayor participación política informada.

Bajo este enfoque, Mercea (2015) afirmó que la información intercambiada en la web sobre políticas regulatorias del internet incrementó el alfabetismo cívico e influyó de forma considerable en la organización de manifestaciones en contra. Por otro lado, en un estudio empírico en los portales de internet del gobierno australiano, Henninger (2017) observó que no es suficiente que las personas cuenten con interés y capacidades de navegación en la web; para acceder a información pública deben generarse conocimientos sobre el funcionamiento de las agencias de gobierno y las reglas de publicación.

De acuerdo con Sturges y Gastinger (2010), el alfabetismo cívico, al igual que el alfabetismo digital, son componentes del alfabetismo informacional; mismo que debe considerar las habilidades para descifrar información sobre las opciones políticas y temas de interés público. Mientras que Skoufias (2014) estudió los impactos de la implementación de las leyes de derecho a la información en el empoderamiento de personas en pobreza, a

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

través de elementos como la participación, el conocimiento cívico, la confianza en las instituciones y la percepción de los servicios públicos.

El vínculo entre el enfoque de capacidades y la participación cívica en instituciones democráticas fue estudiado por Dreze y Sen (2002), quienes establecieron una relación entre el desarrollo humano con el incremento de la participación política en la India. Mientras que Anand (2011) estudió la trascendencia de las legislaciones de derecho a la información en la capacidad de rendir cuentas y la gobernanza de gobiernos locales de distintos países en desarrollo.

De esta manera, se argumenta que, en el estudio del acceso a la información pública y la construcción de políticas de promoción del derecho, resulta necesario revisar las capacidades cívicas de las personas, pues se requiere fomentar interés en los asuntos públicos, el conocimiento de los organismos de gobierno y sus responsabilidades, como herramienta para la participación informada en su comunidad.

Las teorías y evidencias empíricas, antes revisadas, comparten su interés en el estudio de las capacidades y habilidades de las personas para acceder a información pública y hacer uso de ella en el cumplimiento de objetivos. Estas aportaciones fueron consideradas para desarrollar un modelo de análisis de cinco niveles de capacidades y habilidades que, se sugiere, son requeridas para ejercer el DI como una herramienta para la participación cívica, la vigilancia gubernamental y la exigencia de otros derechos humanos.

Es preciso enfatizar que no se argumenta que el ejercicio del DI, o acceder y usar información pública es una capacidad en los términos de la tradición de Sen, sino que es un funcionamiento que requiere una serie de capacidades y habilidades para llevarlo a la práctica. Mientras que se sostiene que el ejercicio del DI como funcionamiento resulta fundamental para el ejercicio de las libertades en el marco de la capacidad de control del entorno político.

El marco analítico propuesto retoma las tres categorías de acceso a la información de las teorías de pobreza informacional (acceso físico, intelectual y social); también se incorporan las capacidades cívicas y las capacidades institucionales de los organismos públicos. Este marco se aplicó en la observación de programas enfocados en promover el DI en comunidades en vulnerabilidad, con la finalidad de identificar las estrategias que pueden ser orientadas al desarrollo de capacidades y habilidades para el acceso y uso de información pública por parte de personas en situación de vulnerabilidad. En la siguiente tabla se detalla el marco analítico y los observables de la investigación.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Tabla 2. Categorías de análisis de las estrategias de promoción del derecho a la información pública

Categorías analíticas (capacidades y habilidades para el ejercicio del DI)	*Observables (estrategias de promoción del DI)*
1. Acceso físico o digital (habilidades para el uso de los medios de información pública)	1.1 Estrategias para garantizar acceso a medios digitales
	1.2 Estrategias de desarrollo de habilidades digitales
2. Acceso informacional o intelectual (habilidades para el procesamiento y análisis de la información)	2.1 Estrategias para el reconocimiento de necesidades de información
	2.2 Estrategias para el desarrollo de habilidades de procesamiento y análisis de la información.
3. Acceso social o comunitario (creencias y actitudes compartidas a la información)	3.1 Estrategias para la modificación de actitudes como desconfianza y escepticismo.
	3.2 Estrategias para el desarrollo de un lenguaje común entre la información pública y la comunidad.
4. Capacidades cívicas (conocimientos y habilidades para la participación política informada)	4.1 Estrategias para fomentar interés y conocimiento de los asuntos públicos.
	4.2 Estrategias de acompañamiento en uso de información en procesos de participación cívica.
5. Capacidades de instituciones públicas para garantizar el DI	5.1 Estrategias de trabajo con organismos garantes y sujetos obligados.

FUENTE: elaboración propia.

V. METODOLOGÍA DE LA INVESTIGACIÓN

En la investigación se utilizó una estrategia de estudio de caso, donde el estudio fue definido por el interés del investigador en el caso específico, y se centró en profundizar sus particularidades, sin buscar su generalización a otros casos (Gerring, 2004; Yin, 2009). Dicho caso fue identificado dentro de un universo de proyectos de organizaciones no gubernamentales, enfocadas en promover el DI en comunidades vulnerables en México, la mayoría

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

de ellas financiadas con esfuerzos públicos, como el programa Prosede, que como fue señalado tienen cortos periodos de implementación y no necesariamente tienen continuidad en sus actividades.

El objetivo del estudio de caso es analizar las estrategias, acciones y herramientas del programa "Transparencia proactiva" de Artículo 19 México y Centroamérica, para identificar aquellas vinculadas al desarrollo de capacidades para el acceso y uso de información pública, con el fin de promover el derecho en comunidades en situación de vulnerabilidad. La selección del estudio de caso responde a que el programa se considera emblemático por el uso de estrategias de intervención comunitaria para promover el uso de información pública en comunidades indígenas.

Es preciso mencionar que la investigación cuenta con un carácter exploratorio, pues está enfocada a discutir la posibilidad del uso del enfoque de capacidades en las políticas de fomento del DI. En este sentido, cobra especial relevancia la selección de estudio de caso, pues permitió obtener una mayor cantidad de observaciones sin buscar que se apliquen en otros contextos.

Las preguntas que orientaron el estudio de caso son: ¿cuáles son las estrategias que utiliza el programa para garantizar el acceso a la información pública de acuerdo con la propuesta de categorías de análisis de niveles de capacidades y habilidades?, ¿qué productos e impactos se han logrado con el desarrollo de esas estrategias?, ¿de qué manera pueden utilizarse esas estrategias en las políticas públicas de promoción del DI en comunidades en vulnerabilidad?

Para el estudio del programa se realizó un análisis documental de informes, minutas, cartas descriptivas, materiales didácticos, videos y otros materiales. También se realizó observación directa en la implementación en campo, en la cual el investigador participó como consultor durante el segundo semestre de 2018.

VI. Análisis del programa "Transparencia proactiva" de Artículo 19 México y Centroamérica

Article 19 es una organización no gubernamental, con sede en Londres, dedicada a promover y defender la libertad de expresión y el derecho a la información. Desde 2015, su oficina regional en México y Centroamérica ha desarrollado el programa Transparencia proactiva, con el apoyo financiero de la William y Flora Hewlett Foundation, con el objetivo de promover el DI en comunidades en vulnerabilidad.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Al principio, la implementación en campo se realizó en alianza con Casa de la Mujer, organización feminista con experiencia territorial en comunidades rurales de Chiapas y Tabasco, en temáticas como salud sexual y reproductiva, derechos de las mujeres, derecho al medio ambiente y territorio. Con esta alianza, se llegó a grupos de mujeres, hablantes de lenguas indígenas, de comunidades rurales que se distinguen por sus altos niveles de analfabetismo y pobreza económica, y bajos niveles de conectividad y escolaridad.[4]

1. *Enfoques, objetivos y propuesta metodológica del programa*

El programa se ha construido con una serie de enfoques que lo diferencian de los proyectos financiados por programas como Prosede, que como ya se dijo, se centra en la sensibilización. Los enfoques mencionados son:

a) Enfoque de DI como derecho llave, para acceder y exigir otros derechos humanos como educación, salud, ambientales e indígenas.
b) Enfoque de intervención comunitaria, para resolver problemas colectivos identificados de manera participativa, difundir el conocimiento compartido en la comunidad e informarles sobre los resultados obtenidos.
c) Enfoque de interseccionalidad, utilizado para reconocer los diferentes niveles de opresión causados por el género, la clase social, la pertenencia a un grupo indígena, entre otros, que limitan el ejercicio de los derechos.
d) Transparencia proactiva, orientada a promover metodologías alternativas para proveer información apropiada, de acuerdo con las necesidades de información de los grupos en vulnerabilidad (Artículo 19, 2017: 31)

El objetivo general del programa es "promover el derecho de acceso a la información para que su uso sirva como herramienta para el ejercicio de

[4] En promedio, el 78% son hablantes de lengua indígena, el 77% de la población de Palenque se encuentra en situación de pobreza y el 33.5% en pobreza extrema; mientras que, en Salto de Agua, los porcentajes de pobreza y pobreza extrema son del 90.9% y el 53.4%. Las personas de las comunidades cuentan con un grado promedio de escolaridad de 5 años, y un analfabetismo de personas mayores de 15 años, en promedio, de 28%: la mayoría de las cuales (64%) son mujeres (Artículo 19, publicación pendiente).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

otros derechos" (Artículo 19, 2017: 29). Mientras que los objetivos específicos se centran en identificar las necesidades de información comunitaria, así como mecanismos alternativos para promover el DI más allá del uso de tecnologías; procurar el acceso a la información para la toma de decisiones de las comunidades, y generar alianzas con organismos garantes del DI para fortalecer sus estrategias de promoción en comunidades en vulnerabilidad (Artículo 19, 2017).

A partir de los resultados, el equipo de implementación de Artículo 19 desarrolló una propuesta metodológica de fomento del DI con un enfoque comunitario, ajustada con la sistematización de sus experiencias en campo. Esta metodología consta de los siguientes doce pasos:

> 1. Identificación participativa de las problemáticas comunitarias.
> 2. Identificación del rol de la información en dichas problemáticas.
> 3. Sensibilización sobre derechos humanos y el derecho a la información en su dimensión individual y social.
> 4. Identificación del tipo de información relevante para cuestionar las problemáticas identificadas, así como de los sujetos obligados […].
> 5. Planteamiento conjunto de preguntas para realizar solicitudes de acceso a la información pertinentes a las problemáticas.
> 6. Ejercicios prácticos de elaboración de solicitudes de acceso a la información y análisis de información publicada en los portales de transparencia.
> 7. Elaboración formal de solicitudes de acceso a la información […] a través de la plataforma [,] o bien, personalmente y por escrito.
> 8. Recepción y sistematización de la información recibida y, en caso de ser necesario, realización de un recurso de revisión […].
> 9. Presentación y entrega de la información con la comunidad.
> 10. Análisis colectivo de la información a la luz de la problemática a resolver.
> 11. Discusión sobre posibles cursos de acción a la luz del análisis colectivo.
> 12. Toma de acción [puede incluir la integración de nuevos actores comunitarios relevantes para la acción a emprender]. (Artículo 19, 2017: 40)

2. *Análisis de las estrategias del programa*

Con esta propuesta metodológica, el equipo de implementación ha realizado distintas acciones de formación como talleres de capacitación de personas multiplicadoras del DI de distintas comunidades y un diplomado de participación ciudadana y derechos humanos para personas jóvenes (Artículo 19,

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

2017). Así como reuniones periódicas de seguimiento en donde se comparte información de interés para las comunidades sobre medio ambiente, violencia contra las mujeres, derechos de los beneficiarios de programas sociales, entre otros.

El programa ha consolidado redes de personas con capacidades y habilidades para el acceso y uso de información pública en distintas comunidades del norte de Chiapas, y a partir de 2018, con personas jóvenes y colectivos de Yucatán. También se han desarrollado materiales didácticos en lenguas indígenas y documentos de sistematización e informes para compartir las metodologías y experiencias.

Por otra parte, se han realizado acciones de réplica en otras zonas; por ejemplo, en alianza con OXFAM México y organizaciones con trabajo territorial en temas como derecho a la salud y cuidado del medio ambiente, se realizaron talleres y pláticas informativas en San Cristóbal de las Casas y San Juan Cancúc, en la zona Altos de Chiapas en 2018. Durante ese año también se iniciaron actividades en el estado de Yucatán, con procesos formativos dirigidos a personas jóvenes, beneficiarias del programa Casa del Niño Indígena, y comités ejidales de distintos municipios.

A continuación, se describen algunas de las estrategias del programa, de acuerdo con el marco analítico de capacidades y habilidades en cinco ámbitos, propuesto por la investigación.

A. *Estrategias de acceso físico. Disminución de las barreras para acceder a información pública disponible en internet*

Debido a las barreras digitales a las que se enfrentan las comunidades, la mayor parte de las solicitudes de información son realizadas por medios electrónicos por el equipo implementador. También se han desarrollado talleres para fortalecer las capacidades digitales y la navegación segura de personas jóvenes, incluyendo el uso de la PNT.

Para fomentar el uso de la PNT, por parte de mujeres que no hablan castellano y no saben escribir, se han ingresado solicitudes de información en formato de audio y en lengua ch'ol. En este caso, tuvieron que pasar varios meses para que el pleno del INAI resolviera ordenar a la Secretaría de Educación Pública atender la solicitud en la lengua ch'ol y en formato de audio.[5]

[5] Recurso de revisión RRA 4434/17, sujeto obligado Secretaría de Educación Pública.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Otra estrategia de alfabetización digital fue la donación de tabletas electrónicas a un colectivo de mujeres, quienes, con ayuda de sus hijos, han aprendido a utilizarlas en la búsqueda de recetas de comida que les sirven para sus actividades económicas. También se realizó un diagnóstico de usabilidad y experiencia de usuarios con una consultoría especializada, con el objetivo de diseñar estrategias orientadas a lograr que las mujeres utilicen los dispositivos por ellas mismas, y para lograr que accedan a información pública.

B. *Estrategias de acceso intelectual. Comprensión del lenguaje burocrático de la información pública*

A partir de la aplicación de herramientas de diagnóstico comunitario, el proyecto realiza acciones de sensibilización para que las personas reconozcan el efecto de la ausencia de información; se busca que las personas conciban los temas de interés comunitario como problemáticas de información, o que pueden ser resueltas con información.

Como parte de la preparación de las acciones de formación y visitas comunitarias, el equipo realiza las labores de discriminación, ordenación y verificación de la validez de la información obtenida. De esta manera, documentos oficiales, como declaraciones de impacto ambiental y reglas de operación de programas sociales, son presentados ante autoridades comunitarias y grupos de mujeres, sin uso de lenguaje técnico, con materiales como esquemas e infografías, y con apoyo de personas traductoras.

C. *Estrategias de acceso social a la información. Disminución de las resistencias hacia la información pública*

El programa aplica estrategias para construir un lenguaje común entre la información pública y las personas participantes, y es desarrollado en conjunto con la comunidad para contar con términos de acceso colectivo. De manera que en algunas comunidades se describió la palabra "derecho" como "lo que nadie nos puede quitar", o la palabra "internet", que fue traducida como "río de conocimientos" en las actividades con jóvenes.

Por otro lado, las estrategias del programa se enfocaron en lograr que las personas pudieran constatar, por ellas mismas o en voz de alguien de su comunidad, que el uso de la información realmente puede tener beneficios. Un ejemplo de esto fue la información obtenida, mediante solicitudes

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

de información, sobre el estatus de dos personas en el padrón beneficiarios del "Programa 70 y más"; en la siguiente visita, las personas de la comunidad asistieron con un listado de alrededor de 15 personas más, interesadas en conocer su estatus en el programa.[6]

En otro caso, mujeres beneficiarias del programa Prospera denunciaron ser víctimas de coacción por parte de los promotores, quienes condicionaban la entrega de sus apoyos con la compra de chocolates de marca *Ensure*. A través de una solicitud de información, las mujeres conocieron la ilegalidad de esta práctica y se negaron a comprar el producto, fomentando en otras mujeres beneficiarias a su rechazo.[7]

D. *Los elementos cívicos en el uso de información pública. Impulso a la participación política informada*

El programa ofrece acompañamiento a las personas participantes, para el uso de la información pública en procesos de participación comunitaria y rendición de cuentas; además, se pone especial atención en que las personas conozcan los sujetos obligados a los que se solicita la información, los organismos garantes del DI y sus responsabilidades.

Ahora bien, el prototipo de metodología de intervención, desarrollada por el programa, concluye con acciones específicas para el uso de información. Un ejemplo de esto es el caso de la comunidad Lázaro Cárdenas, que mediante una solicitud de información pudo denunciar ante la Secretaría de Salud del Estado el incumplimiento de los horarios de atención y la gratuidad del servicio por parte del personal médico.[8] Las mujeres de esta comunidad conformaron un grupo de seguimiento y vigilancia a la correcta operación del centro de salud, las actividades del personal y los medicamentos disponibles.

Otro ejemplo de acompañamiento en el uso de información fue el que se llevó a cabo con autoridades ejidales del valle de Tulijá durante 2016.[9] A partir de información obtenida por solicitudes, se pidió una audiencia

[6] Solicitud de información con folio 2000100011618, dirigida a Coordinación Nacional de Prospera Programa de Inclusión Social.

[7] Solicitud de información con folio 2000100014216, dirigida a Coordinación Nacional de Prospera Programa de Inclusión Social.

[8] Este caso de éxito, en el uso de información pública, se encuentra plasmado en el cuento "Francisca y la información, derecho a la información para la salud".

[9] Este caso de éxito, en el uso de información pública, se encuentra plasmado en el cuento "Felipe y la información, derecho a la información y derecho al territorio".

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

pública con las autoridades del municipio de Salto de Agua para pedir cuentas sobre los megaproyectos en construcción en los territorios de las comunidades.

E. *Capacidades de sujetos obligados y organismos garantes para asegurar el acceso a la información*

El programa reconoce la importancia del desempeño de los sujetos obligados, y ha realizado acercamientos con organismos garantes locales de Chiapas y Tabasco para asegurar el derecho a la información pública sin discriminación, aunque no se logró una colaboración más amplia. No obstante, en 2019 se logró el establecimiento de un convenio de colaboración con el Instituto Estatal de Acceso a la Información Pública, Yucatán, para promover el derecho en comunidades indígenas del estado.

En conclusión, el programa se enfoca en desarrollar estrategias encaminadas a desarrollar y fortalecer capacidades en las comunidades para acceder y utilizar la información pública. Bajo un enfoque de intervención comunitaria, se pone atención en las necesidades comunitarias, y en el acompañamiento de las personas en el proceso de acceso y uso de la información para resolver problemas y exigir sus derechos humanos.

Ahora bien, el programa reconoce que alcanzar capacidades en las comunidades es un proceso más amplio que podría materializarse en fases avanzadas. También es consciente de otros desafíos, como la necesidad de traducir la información pública a un lenguaje menos complejo, aumentar las capacidades y la disposición de las instituciones públicas, y contrarrestar las dinámicas de los grupos de poder locales que limitan el acceso a la información (Artículo 19, 2017: 45-49).

Es importante mencionar que también se identifican algunas áreas de oportunidad para mejorar las acciones, tales como el desarrollo de evaluaciones de impacto y resultados para evidenciar su efectividad y hacer ajustes, si es el caso. Otra área de oportunidad es el desarrollo de estrategias para limitar la dependencia de las comunidades a las visitas de seguimiento del equipo implementador, y diseñar formas para dar sostenibilidad a las acciones con alianzas locales.

Futuras investigaciones deben comprobar la efectividad de las estrategias identificadas para el desarrollo de capacidades y habilidades, por medio de evaluaciones de productos e impactos del programa como los realizados por Zermeño (2010) y Skoufias (2014).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

VII. Propuestas para mejorar la política de promoción del derecho a la información desde el enfoque de capacidades

Mediante los enfoques señalados anteriormente, y considerando los hallazgos del estudio de caso, se propone que las políticas públicas de promoción del DI se deben orientar a desarrollar capacidades y habilidades que permitan a las personas acceder y utilizar información pública. El enfoque de capacidades permitirá poner especial atención en las personas y los elementos contextuales que favorezcan el ejercicio del derecho.

Por otro lado, el enfoque de capacidades representa una alternativa para reorientar las acciones basadas en formación de usuarios, reconociendo el hecho de que el objetivo de las políticas de promoción no es únicamente que las personas realicen solicitudes de información o visitas a los portales de transparencia. Es necesario promover el uso del derecho como medio para la vigilancia gubernamental, el ejercicio de otros derechos y la participación en los asuntos públicos. No se trata de limitarse a formar personas "usuarias", sino que el uso de la información pública tenga impactos personales o comunitarios.

Con base en las observaciones anteriores, a continuación, se ofrecen algunas propuestas para fortalecer la política pública de promoción del DI, con base en el enfoque de capacidades, que posibilite el acceso y uso de información pública a las personas en situación de vulnerabilidad.

1) Buscar medios de acceso, alternativos a los digitales, para acercar información pública a las personas con brechas como el lenguaje o la alfabetización; colaborar con centros educativos y demás espacios públicos con conexión a internet para la difusión de información pública.
2) Transformar las preocupaciones y necesidades de las personas y comunidades en problemas de ausencia de información; ofrecer acompañamiento en el procesamiento y análisis de la información pública obtenida.
3) Usar estrategias de intervención comunitaria para explicar conceptos de manera accesible y en la lengua de las personas. Buscar que las mismas personas de las comunidades se conviertan en difusoras de experiencias exitosas en el uso de información pública.
4) Promover que las personas identifiquen las responsabilidades de los organismos de gobierno en la garantía de su DI. Ofrecer acom-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

pañamiento para el uso de la información pública en procesos de participación comunitaria y rendición de cuentas.

5) Realizar acciones con funcionarios de sujetos obligados y organismos garantes para facilitar el ejercicio del derecho, generar y compartir información de calidad, focalizada y útil, a los grupos de la población en situación de vulnerabilidad.

VIII. Reflexiones finales

En la era informacional, el DI es una herramienta valiosa para el desarrollo humano y la participación política de las personas. Aun cuando México cuenta con una legislación reconocida a nivel mundial, el enfoque de promoción masiva y formación de usuarios en las políticas promoción del DI no han logrado trascendencia en las personas en situación de vulnerabilidad, por lo que se deben construir políticas públicas que atiendan las múltiples barreras que dificultan a ciertos grupos acceder y utilizar información pública.

Ahora bien, la promoción no debería enfocarse únicamente en cumplir con la obligación de lograr más "usuarios" o un mayor conocimiento del derecho, se debe reconocer que hay personas que, por limitaciones del lenguaje, de alfabetismo o conectividad, difícilmente podrán convertirse en usuarias de las plataformas de acceso y consulta de información pública. Además, aun cuando se logre derribar las barreras y realizar una solicitud o una consulta, todavía existe un largo camino para validar, interpretar y usar esa información. Es por ello que se debe poner especial atención en el acompañamiento en el uso de la información pública como herramienta para la solución de problemáticas comunitarias y la exigencia de otros derechos humanos.

Por otro lado, las acciones con poblaciones objetivo deben basarse en diagnósticos comunitarios que muestren las problemáticas de interés de las personas, y sean sensibles a sus contextos particulares y a las barreras de distintos tipos que les dificultan el acceso y uso de información pública. De manera que se debe poner especial atención en desarrollar intervenciones centradas en las personas y las barreras educativas, de género, pertenencia a un grupo indígena, entre otras, para beneficiarse de la información pública.

Es preciso mencionar que los esfuerzos de socialización se verán limitados si no se desarrollan acciones sistemáticas para lograr que los sujetos obligados faciliten la entrega de información pública de interés para las

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

personas en vulnerabilidad. Es importante buscar los medios y formatos idóneos, más allá de los digitales, para compartir información sobre programas sociales, derecho a la salud y la educación, medio ambiente y territorio, entre otros temas recurrentes en el estudio de caso, más allá de las páginas de internet a las que muchas personas no tienen acceso.

Con estas consideraciones y el desarrollo de herramientas para evaluar procesos, productos e impactos, se lograría el objetivo de promover el derecho a la información en personas en vulnerabilidad, como una herramienta de utilidad para el desarrollo humano, la participación ciudadana y la rendición de cuentas.

IX. Bibliografía

Abramovich, Víctor y Courtis, Christian, 2000, *El acceso a la información como derecho,* CELS, Buenos Aires, disponible en *http://goo.gl/SmigVE*, consultado el 20 de junio de 2015.

Anand, P. B., 2011, "Right to Information and Local Government: an Exploration", *Journal of Human Development and Capabilities*, vol. 12, núm. 1.

Basu, K. y López-Calva, L., 2010, "Functionings and Capabilities", en Arrow, K. *et al*. (eds.), *Handbook of Social Choice and Welfare*, vol. 2, Elsevier Science, North Holland.

Bawden, David, 2001, "Information and Digital Literacies: a Review of Concepts", *Journal of Documentation*, vol. 57, núm. 2.

Bovens, Mark, 2002, "Information Rights: Citizenship in the Information Society", *The Journal of Political Philosophy*, vol. 10, núm. 3.

Britz, J. J., 2004, "To Know or Not to Know: a Moral Reflection on Information Poverty", *Journal of Information Science*, vol. 30, núm. 3.

Britz, J. J. y Blignaut, J. N., 2001, "Information Poverty and Social Justice", *South African Journal of Library & Information Science*, 02568861, vol. 67, núm. 2.

Burnett, G. *et al*., 2008, "Normative Behaviour and Information: The Social Aspects of Information Access", *Library and Information Science Research*, núm. 30.

Campbell, B., 1990, "What is literacy? Acquiring and Using Literacy Skills", *Australasian Public Libraries and Information Services*, núm. 3.

Castells, Manuel, 1997, *Vol. I. La sociedad red*, Madrid, Alianza Editorial.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Chatman, E. A., 2000, "Framing Social Life in Theory and Research", *The New Review of Information Behaviour Research*, núm. 1.

Childers, T. y Post, J. A., 1975, *The Information-Poor in America*, Metuchen, New Jersey, Scarecrow Press.

Deneulin, S. y Stewart, F., 2002, "Amartya Sen's Contribution to Development Thinking", *Studies in Comparative International Development*, vol. 37, núm. 2.

Doyle, Christina S., 1994, *Information Literacy in an Information Society: a Concept for the Information Age*, Syracuse, Nueva York, ERIC Clearinghouse.

Dreze, J. y Sen, A., 2002, *India — Development and Participation*, Oxford, Oxford University Press.

Eshet-Alkalai, Yoram, 2004, "Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era", *Journal of Educational Multimedia and Hypermedia*, vol. 13, núm. 1.

Fukuda-Parr, S., 2003, "The Human Development Paradigm: Operationalizing Sen's Ideas on Capabilities", *Feminist Economics*, vol. 9, núm. 2/3.

Gerring, John, 2004, "What is a Case Study and What is it Good For?", *The American Political Science Review*, vol. 98, núm. 2.

Guerrero-Amparán, J. P. y Sepúlveda Toledo, M., 2009, *The Right to Information for Marginalized Groups. The Experience of* Proyecto Comunidades *in Mexico 2005-2007*, México, William and Flora Hewlett Packard Foundation.

Henninger, Maureen, 2017, "Government Information: Literacies, Behaviours and Practices", *Government Information Quarterly*, vol. 34, núm. 1.

Hersberger, J. A., 2002-2003, "Are the Economically Poor Information Poor? Does the Digital Divide affect the Homeless and Access to Information?", *Canadian Journal of Information and Library Science*, vol. 27, núm. 3.

Luna Pla, Issa, 2013, "Empoderamiento pro-desarrollo humano con información pública", *Derecho Comparado de la Información*, núm. 21.

Luna Pla, Issa, 2012, "Pobreza informacional y el derecho de acceso a la información pública. Un problema de capacidades", *Transparencia y Privacidad. Revista Mexicana de Acceso a la Información y Protección de Datos*, núm. 2.

Mercea, Dan, 2015, "Making Sense of Democratic Institutions Intertextually: Communication on Social Media as a Civic Literacy Event Preceding Collective Action", *The Communication Review*, vol. 18, núm. 13.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

MILNER, Henry, 2002, *Civic Literacy: How Informed Citizens Make Democracy Works*, Hanover, NH, University Press of New England.

NUSSBAUM, Martha, 2012, *Crear capacidades: propuesta para el desarrollo humano*, Barcelona, Paidós.

NUSSBAUM, Martha, 2011, "Education and Democratic Citizenship: Capabilities and Quality Education", *Journal of Human Development*, vol. 7, núm. 3.

NUSSBAUM, Martha, 2004, "Promoting Women's Capabilities", en BENARIA, Lourdes y BISNATH, Savitri (eds.), *Global Tensions: Challenges and Opportunities in the World Economy*, Routledge.

NUSSBAUM, Martha, 2003, "Capabilities as Fundamental Entitlements: Sen and Social Justice", *Feminist Economics*, vol. 9, núm. 2-3.

NUSSBAUM, Martha, 2000, *Women and Human Development. The Capabilities Approach*, Cambridge University Press.

RÍOS ORTEGA, Jaime, 2017, *De la información a la sociedad y de la sociedad a la información*, México, UASLP, Centro de Documentación Histórica Rafael Montejano y Aguiñaga.

ROBEYNS, Ingrid, 2005, "The Capability Approach: a Theoretical Survey", *Journal of Human Development*, vol. 6, núm. 1.

SAITH, Ruhi, 2001, "Capabilities: the Concept and its Operationalization", *Queen Elizabeth House Working Paper 66*, Oxford, Oxford University.

SANDOVAL B., Irma E., 2013, "Hacia un proyecto "democrático-expansivo" de transparencia", *Revista Mexicana de Ciencias Políticas y Sociales*, vol. 58, núm. 219.

SEN, Amartya, 2016, *La desigualdad económica*, México, Fondo de Cultura Económica.

SEN, Amartya, 2005, "Human Rights and Capabilities", *Journal of Human Development*, vol. 6, núm. 20.

SEN, Amartya, 2004, "Capabilities, Lists, and Public Reason: Continuing the Conversation", *Feminist Economics*, vol. 10, núm. 3.

SEN, Amartya, 2004, "Elements of a Theory of Human Rights", *Philosophy & Public Affairs*, vol. 32, núm. 4.

SEN, Amartya, 2000, *Desarrollo y libertad*, Buenos Aires, Planeta.

SKOUFIAS, E. *et al*., 2014, "Does Access to Information Empower the Poor? Evidence from the Dominican Republic", *Policy Research Working Paper* (6895), Washington, DC, World Bank Group.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Stiglitz, Joseph E., 2002, "La información y el cambio en el paradigma de la ciencia económica", *Revista Asturiana de Economía*, núm. 25.

Stiglitz, Joseph E., 1999, "On Liberty, the Right to Know and Public Discourse: The Role of Transparency in Public Life", en Gibney, M. (ed.), *Globalizing Rights*, Oxford, Oxford University Press.

Sturges, Paul y Gastinger, A., 2010, "Information Literacy as a Human Right", *International Journal of Libraries and Information Studies*, vol. 60, núm. 3.

Thompson, Kim, 2007, "Furthering Understanding of Information Literacy through the Social Study of Information Poverty", *The Canadian Journal of Information and Library Science*, vol. 31, núm. 1.

Urquijo Angarita, Martín, 2014, "La teoría de las capacidades en Amartya Sen", *Edetania. Estudios y Propuestas Socioeducativas*, núm. 46.

Yin, Robert K., 2009, *Case Study Research: Design and Methods*, California, SAGE Publication Inc.

Zermeño, N. F. *et al*., 2010, *El acceso a la información en comunidades marginadas*, México, UNAM-EPADEQ.

1. *Documentos*

Access Info Europe and the Centre for Law and Democracy, 2016, "Índice global del derecho a la información", disponible en *www.rti-rating.org/*.

Artículo 19 México Centroamérica, "Informe bianual del proyecto Transparencia proactiva" (publicación pendiente).

Artículo 19, 2017, "Transparencia proactiva: informe de *Article 19* y Casa de la Mujer Ixim Antsetic".

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2018, "Plan nacional de socialización del derecho de acceso a la información", México, consultado en *http://proyectos.inai.org.mx/plandai/*.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2005, "Informe mundial de la UNESCO: hacia las sociedades del conocimiento", París, UNESCO.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), 2003, Declaración de Principios, Cumbre Mundial sobre la Sociedad de la Información, Ginebra, Suiza.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Programa de Naciones Unidas para el Desarrollo (PNUD), 2004, "Informe sobre desarrollo humano 2004" , Madrid, Ediciones Mundi Prensa.

Programa de Naciones Unidas para el Desarrollo, "Desarrollo de capacidades. Texto básico del PNUD", disponible en *https://goo.gl/4zXEzw.*

Programa de Naciones Unidas para el Desarrollo, "La verdadera riqueza de las naciones: Caminos al desarrollo humano. Informe sobre Desarrollo Humano 2010", disponible en *https://goo.gl/MeFsq4*.

Sistema Nacional de Transparencia, 2017, Programa Nacional de Transparencia y Acceso a la Información 2017-2021, consultado en *https://bit.ly/2Ijp5AF.*

2. *Videos*

Artículo 19 México y Centroamérica, 2015a, "Derecho a la información para las mujeres", disponible en *https://goo.gl/MVF8VQ*.

Artículo 19 México y Centroamérica, 2015b, "Cuando la información cura", disponible en *https://goo.gl/mXSXc3*.

Artículo 19 México y Centroamérica, 2016a, "La información somos todas y todos", disponible en *https://goo.gl/jsem3A*.

Artículo 19 México y Centroamérica, 2016b, "Red Junco: la voz de nuestros pueblos", disponible en *https://goo.gl/dE9Hpg*.

Artículo 19 México y Centroamérica, 2017b, "DAI Tejiendo comunidad", disponible en *https://goo.gl/P9SPmy*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Comentarios jurídicos

Universidad Nacional Autónoma de México, IIJ-BJV, 2020
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

ANÁLISIS SOBRE LA CORRECCIÓN DE DATOS PERSONALES EN LA PLATAFORMA MÉXICO

ANALYSIS ON THE CORRECTION OF PERSONAL DATA IN THE MEXICO PLATFORM

Rafael MARTÍNEZ PUÓN*

RESUMEN. En ocasiones, el Estado vulnera la vida privada y la intimidad de las personas frente a la acumulación excesiva de datos personales de sus instituciones de seguridad pública; este es el caso de un ciudadano cuyos datos personales estaban registrados en una base de datos denominada Plataforma México y eso le causaba una afectación en su vida personal y profesional al impedirle el acceso a un empleo. El ciudadano pidió al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública el retiro de sus datos personales de esa base de datos, su solicitud fue negada. La persona ejerció su derecho y recurrió al entonces Instituto Federal de Acceso a la Información Pública, expediente: RPD 0507/14. Algunas de las principales aportaciones del texto son: los datos personales pueden ser vulnerados si la autoridad no tiene el suficiente cuidado; la acumulación de información a través del uso de la tecnología puede conllevar el riesgo de violaciones a la privacidad si no existe un adecuado manejo; se requiere proteger los derechos de las personas, sean de privacidad y/o de acceso a la información, y al mismo tiempo permitir que su uso guarde proporcionalidad respecto del interés público de hacer pública la información.

* Doctor en Gobierno y administración pública por el Instituto Universitario Ortega y Gasset adscrito a la Universidad Complutense de Madrid. Investigador del Sistema Nacional de Investigadores nivel II. Miembro fundador del Consejo Consultivo del INAI. Director de la *Revista Buen Gobierno*. *rmartinez@inap.org.mx*.

Fecha de recepción: 06 de octubre de 2019.
Fecha de dictamen: 27 de noviembre de 2019.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

PALABRAS CLAVE. Protección de datos personales, seguridad pública, derechos ARCO, Plataforma México.

ABSTRACT. This article is relevant because sometimes the State violates people's privacy and their intimacy due to personal data excessive accumulation from their public security institutions; such is the case of a citizen whose personal data were registered in a database called Mexico Platform. This affected him in his personal and professional life by preventing him from accessing a job. The citizen asked the Executive Secretariat of the National Public Security System to remove his personal data from that database, his request was denied. The person exercised his right and resorted to the former Federal Institute of Access to Public Information, file: RPD 0507/14. Some of the main contributions of the article are: personal data may be violated if the authority is not careful enough; the accumulation of information through the use of technology may carry the risk of privacy violations unless proper management exists; it is necessary to protect the rights of people, whether the right to privacy and/or access to information and at the same time allow their use to be proportional to the public interest of making the information public.

KEYWORDS. Personal data protection, public security, ARCO rights, Mexico Platform.

I. Introducción

En México, los derechos de acceso a la información pública y protección de datos personales encuentran su primer antecedente en la Ley General de Protección y Equilibrio Ecológico de 1988,[1] como respuesta a las recomendaciones establecidas en la Declaración de la Conferencia de las Naciones Unidas sobre Medio Ambiente y Desarrollo de 1972; sin embargo, el primero de éstos fue reconocido en nuestro país hasta la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), publicada en el *Diario Oficial de la Federación* el

[1] Poder Ejecutivo Federal, 1988, Ley General del Equilibrio Ecológico y la Protección al Ambiente, *Diario Oficial de la Federación*, 28 de enero, disponible en *https://www.dof.gob.mx/nota_detalle.php?codigo=4718573&fecha=28/01/1988*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

11 de junio de 2002, convirtiéndose en el primer instrumento normativo a nivel nacional que estableció los mecanismos para garantizar el ejercicio del derecho de acceso a la información pública en el ámbito gubernamental; derecho que adquirió rango constitucional a través de la reforma al artículo 6o. de la Constitución (2007), y que provocó el posterior reconocimiento al derecho de protección de datos personales consagrado en el artículo 16 de dicho ordenamiento (2009).

De esta manera podemos advertir que el ejercicio de los derechos de acceso a la información pública y protección de datos personales han evolucionado hasta su reconocimiento y garantía a nivel nacional, resolviendo en el camino uno de los grandes inconvenientes en el ejercicio de dichos derechos, como lo fue la falta de instrumentos normativos que homologaran el ejercicio de los mismos en todo el país, lo que impedía poder garantizar los derechos de acceso, rectificación, cancelación y oposición en el sector público de manera plena. Problema que fue superado, primero, con la expedición de la Ley General de Transparencia y Acceso a la Información Pública (2015), y posteriormente, con la entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017). Con el objeto de ilustrar esta afirmación, estudiaremos una resolución del pleno del otrora Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI), relacionada con la seguridad pública y el ejercicio de los derechos de acceso a la información pública y protección de datos personales.

El caso por revisar es el de una persona que solicitó en 2013 al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) sus datos personales registrados en la Plataforma México (red nacional que alberga las bases de datos criminalísticas y de personal de seguridad pública), así como la cancelación de éstos, ya que a su parecer le causaba una clara afectación en su vida personal y profesional. La respuesta que recibió fue una negativa, argumentando la falta de competencia del propio Secretariado, sin orientarlo a la instancia que sí lo era. Ante tal circunstancia, dicha persona interpuso un recurso de impugnación ante el entonces IFAI, con el objeto de conseguir una respuesta acorde con el ejercicio de su derecho a la protección de datos personales.

¿Por qué es pertinente analizar este caso cuando ocurrió en 2013? Porque es un tema que sigue siendo actual, pues en el imperativo de combatir el crimen por parte del Estado mexicano, en ocasiones se vulnera la vida privada y la intimidad de las personas frente a la acumulación excesiva de datos personales por parte de las instituciones de seguridad pública responsables de hacer cumplir la ley. Si bien el combate contra el crimen

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

requiere de soluciones expeditas y efectivas, éstas no pueden pasar por encima de la dignidad de las personas.

El análisis del caso se divide en tres partes: la primera parte comprende un repaso de los elementos que vinculan el "deber ser" de la seguridad pública en relación con el respeto de los derechos humanos, y de cómo se ha problematizado la seguridad, debido a factores de violencia y combate al crimen que derivan en ataques, por decirlo de alguna forma, a los derechos y libertades de las personas: como es el caso de la vulneración de la privacidad e intimidad de las personas, y por ende, de la información que las instituciones de seguridad pública detentan de éstas. En la segunda parte, se describe el caso de los datos personales contenidos en la Plataforma México, y de cómo resolvió el entonces IFAI, pues en lo general favoreció a la persona titular de dichos datos personales. En la tercera parte, se formulan algunos comentarios sobre el problema jurídico de fondo y las reflexiones a las que se llegó, en relación con los posibles retos que enfrenta el ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

II. Desarrollo

1. *Seguridad pública y derechos humanos*

La seguridad pública se relaciona directamente con la creación del Estado de derecho; en otras palabras, la obligación del Estado de garantizar las libertades proclamadas a finales del siglo XVIII con la Revolución francesa. Puesto que el diseño del espacio público-político, desde ese momento histórico, aspira a ser uno en el que la violencia no sea una forma de relacionarse en sociedad, pensemos en la antigua referencia de la "ley del más fuerte", un fin práctico que asegure la convivencia pacífica necesaria para llevar a cabo de manera satisfactoria tareas más complejas como la regulación de la vida social, la parcelación de las libertades, la prestación de los servicios públicos o la redistribución del ingreso (Gallego, 2004).

Entonces, la seguridad pública ejerce la función de tutela del orden y la paz pública, teniendo como fin la conservación del Estado de derecho, lo cual implica un alto grado de complejidad o dificultad para quienes lo ejercen, ya que mantener la paz y el orden, sin afectar los derechos y las libertades de los individuos, no es un reto menor. Moreno (2004) destaca como el reto principal de las instituciones encargadas de la seguridad pú-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

blica, el lograr un equilibrio entre la coercibilidad de las normas jurídicas sin faltar al respeto de los derechos y valores fundamentales en el ejercicio de sus funciones, por ejemplo, proteger la integridad física de las personas y sus bienes, prevenir la comisión de delitos e infracciones a las normas, colaborar en la investigación y persecución de los delitos, y auxiliar a la población en caso de siniestro o desastre, siendo estas actividades fundamentales para la estabilidad de una nación; a la par tiene un "talón de Aquiles", ya que si alguien falla o varios fallan se propicia un efecto dominó que podría tener consecuencias negativas en la población, y que hoy en México nos flagela día con día.

De ese modo, la seguridad pública debería proveer de un clima de tranquilidad (un estado de paz) y seguridad para lograr el desarrollo como seres humanos, seguido de una búsqueda continua del fortalecimiento del vínculo indisoluble de la seguridad pública con los derechos humanos y su debida protección por parte de las autoridades estatales, y bajo un esquema de valores, los cuales comprendan como prioritarios: el respeto a la vida y a la integridad de las personas, y a sus derechos y libertades. Además de la garantía de que las personas también serán protegidas frente al Estado, preservando y tutelando sus libertades y derechos humanos.

Es importante recordar que en el Estado mexicano los derechos humanos se garantizan en la Constitución, y mediante la reforma constitucional del 10 de junio de 2011 se generó un reconocimiento expreso de tales derechos; es así que los derechos humanos se configuraron a través de una doble fuente: por un lado, la propia Constitución, y por otro, los tratados internacionales, de los que el Estado mexicano sea parte. Aunque se encontraban reconocidos conforme a lo dispuesto en el artículo 133 de nuestra carta magna, el mérito de la reforma fue despejar cualquier duda sobre su vigencia y promover su conocimiento, interpretación y aplicación (Ovalle, 2016).

Así podemos destacar que cualquier entidad estatal que tenga facultades, sean administrativas o judiciales en nuestro país, se encuentra obligada —tratándose de derechos humanos— a favorecer su reconocimiento o ejercicio.

El principio fundamental para interpretar los derechos humanos (principio propersona, al que también suelen llamar *pro homine*), al cual se refiere el segundo párrafo del artículo 1o., dispone que las normas sobre derechos humanos "se interpretarán de conformidad con la Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a todas las personas con la protección más amplia" (Ovalle, 2016, p. 163).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Una vez repasados estos aspectos sobre el vínculo de la seguridad pública y el respeto a los derechos humanos, se considera pertinente no perder de vista:

- La noción de seguridad pública, como hemos apuntado, va más allá de referirse a la actividad policial y de los organismos especializados en la prevención, detección e investigación de los delitos.
- El combate contra el crimen no puede ubicarse al margen del respeto y/o reconocimiento de los derechos humanos.
- La actividad estatal no debe entrometerse en la vida de las personas más allá de lo que se considere como indispensable para el desempeño de sus funciones.
- En México, como en cualquier democracia constitucional, la seguridad pública debe ser el medio institucional que asegure a toda persona del goce y disfrute de sus derechos.

Es necesario reconocer que existe una serie de condiciones que nos permiten repensar la relación que tiene la seguridad pública y los derechos humanos, y de cómo mantenerla. Moreno (2004) afirma que las principales violaciones a los derechos humanos, precisamente son ejecutadas por las personas encargadas de la seguridad pública, en especial, la policía en todas sus modalidades y en la mayoría de los países; y, según el Estado de que se trate, existe una latente violación a los derechos sociales en general, a los ecológicos, a la autodeterminación de los pueblos, así como a los de las personas adultas mayores, de los menores de edad, de las mujeres, de las personas con discapacidad o de los migrantes.

En este sentido, cabe retomar lo que Ferrajoli (2001) plantea en su *Teoría del garantismo* sobre generar un nuevo modelo normativo del derecho, en donde el sistema de poder sea mínimo, y se piense a los derechos fundamentales como "límites" a través de los cuales se maximiza la libertad y se minimiza la arbitrariedad e impunidad por parte de los gobernantes; vale la pena recordar que está discusión en nuestro país no es nueva, ya hace más de 10 años se ha venido discutiendo esta posición de Ferrajoli (2001), en razón de garantizar (vía garantías procesales) en un sentido más amplio el ejercicio de los derechos fundamentales sobre el ejercicio del poder, apoyando la idea de favorecer la "ley del más débil".

Ahora bien, la otra cara de la moneda es la siguiente: de acuerdo con los datos proporcionados por México Evalúa, el 2017 fue considerado el año más violento de la historia mexicana reciente, ya que, durante el mandato del presidente Enrique Peña Nieto, ningún año registró menos de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

20 mil homicidios dolosos (aunque 2014 y 2015 fueron menos violentos). Cabría destacar que el factor central de la violencia es la proliferación de armas de fuego en México, ya que con base en datos del SESNSP (2018b), en 2017, el 68% de los homicidios dolosos (16 898) se cometieron con armas de fuego, y las mismas armas provocaron 8486 lesiones dolosas. Estos datos indican que, durante un periodo considerable, la política pública contra el crimen se endureció, y es por esto que se insistió, desde el mandato de Felipe Calderón Hinojosa, en que se impulsara la integración de la denominada Plataforma México, que es parte del tema central de nuestro caso.

López Portillo y Barrena (2008) estiman que, en este tipo de contexto, el Estado policía representa un conjunto de problemas, pues con la idea de combatir al crimen se vulnera la vida privada y la intimidad de las personas debido a la acumulación excesiva de datos personales por parte de las fuerzas encargadas de hacer cumplir la ley. En otras palabras, el combate contra el crimen requiere eficiencia y eficacia, pero no puede pasar por encima de la dignidad, de los derechos y de las libertades de las personas. Es por esto que nuestro caso sobre la Plataforma México cobra relevancia.

2. *Descripción del caso "Datos personales en la Plataforma México"*

A continuación, revisaremos brevemente cuáles fueron las circunstancias que desembocaron en la negativa a corregir o cancelar la información contenida en las bases de datos del Centro Nacional de Información del Sistema Nacional de Seguridad Pública por parte del sujeto obligado, y que causaba perjuicio a la persona titular de los datos personales.

A. *Datos generales del caso*

IFAI, Expediente: RPD 0507/14, comisionado ponente: Joel Salas Suárez, sesión del pleno del 6 de agosto de 2014, Ciudad de México.

B. *Descripción de los hechos*

Una persona manifestó que en 2013 deseaba laborar en el ámbito de seguridad pública en el Municipio de Juárez, Nuevo León, y durante su proceso de incorporación le informaron que existía información de su per-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

sona en la denominada Plataforma México. Lo que le causó inquietud y procedió a comunicarse con el Departamento de Acceso a la Información Pública del Municipio de Acámbaro, Guanajuato, para conocer el tipo de información de que se trataba; sin embargo, el Municipio le informó su desconocimiento sobre el tipo de información contenida en dicha Plataforma. A la par, solicitó las cartas de no antecedentes penales y de no inhabilitación, las cuales le fueron entregadas sin ningún problema.

C. *Solicitud al sujeto obligado*

El particular solicitó al SESNSP le fuera informado qué tipo de datos personales estaban contenidos sobre su persona en la Plataforma México, así como la cancelación de dicha información en el registro.

D. *Respuesta del sujeto obligado*

La respuesta del SESNSP se realizó con base a lo siguiente:

- Que la solicitud fue turnada al Centro Nacional de Información, el cual indicó su competencia únicamente de la *operación* del Sistema Nacional de Información de Seguridad Pública, así como del establecimiento, control, administración y resguardo de las bases de datos criminalísticas y de personal de seguridad pública.
- Que los artículos 109 y 117, de la Ley General del Sistema Nacional de Seguridad Pública del 2 de enero de 2009, establecen que serán la Federación, los estados, el Distrito Federal (hoy Ciudad de México) y los municipios, los responsables de suministrar, intercambiar, sistematizar, *consultar, analizar y actualizar* la información que diariamente se genere sobre seguridad pública; y de integrar y actualizar el Sistema Único de Información Criminal (SUIC) con la información que generen las instituciones de procuración de justicia e instituciones de seguridad pública.
- Que había falta de claridad sobre los documentos solicitados.
- Que la información sobre elementos policiales o de seguridad pública contenida en la base de datos del Registro Nacional de Personal de Seguridad Pública, no era información concerniente a una persona física identificada o identificable por lo que no constituían datos personales.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

- Expresó no contar con atribuciones para corregir o cancelar la información de las bases de datos del Sistema Nacional de Información de Seguridad Pública, ni tampoco de los datos personales contenidos en el Registro Nacional de Personal de Seguridad Pública, encontrándose imposibilitado jurídicamente para efectuar la corrección solicitada.

E. *Inconformidad*

El particular interpuso su recurso de revisión sobre la respuesta obtenida por el SESNSP, pues consideró que al requerir la rectificación y cancelación de sus datos personales no debía existir impedimento o reserva legal alguna para negarle su solicitud.

F. *Argumentos para el fortalecimiento de la decisión y resolución del pleno*

En la resolución del expediente, no quedaba claro si existía la posibilidad de que los datos a los que hacía referencia el particular tenían que ver o no con datos personales, como se argumentaba de inicio, puesto que la institución de seguridad pública de Nuevo León no le otorgó mayores detalles a la persona, por lo que en diligencias para mejor proveer, el comisionado ponente requirió al SESNSP información adicional a la manifestada con anterioridad, por tanto, el IFAI se allegó de la siguiente información, la cual se consideró determinante en la formulación del proyecto de resolución presentado al pleno:

1) Si cuenta o no con datos personales del particular y, de ser así, especificara cuáles son, así como la base de datos en donde se encuentran.

La respuesta fue positiva, al señalar que *en el Registro Nacional de Personal de Seguridad Pública se encuentran inscritos datos personales del particular como: nombre, lugar de nacimiento, fecha de nacimiento, sexo y Registro Federal de Contribuyentes.*

2) Describiera el tipo de información que se resguarda en la Plataforma México.

Manifestó que *el Centro Nacional de Información del SESNSP resguarda las bases de datos criminalísticas y de personal de seguridad pública, que contienen registros o información relacionada con detenciones, información*

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

criminal, personal de seguridad pública, servicios de seguridad privada, armamento, equipo, vehículos, huellas dactilares, teléfonos celulares, sentenciados y las demás necesarias para la operación del Sistema.

3) Señalara cuál es el ente que se encarga de la administración, específicamente de incorporar y en su caso de *eliminar datos* de la Plataforma México.

Indicó que conforme a lo dispuesto en el artículo 19, fracción I, de la Ley General del Sistema Nacional de Seguridad Pública, la administración de las bases de datos criminalística y de *personal de seguridad pública*, *corresponde al Centro Nacional de Información.*

4) Mencionara cuál es la normativa que regula el funcionamiento y las particularidades de la Plataforma México. En su caso remita dicho marco normativo.

Al respecto respondió que no era de su conocimiento o competencia informar cuál era la normativa que regula el *funcionamiento y las particularidades* de la Plataforma México.

5) Explicara las razones por las cuales considera que no cuenta con atribuciones para corregir o cancelar datos personales.

Destacó encontrarse jurídica y materialmente imposibilitado para corregir o cancelar datos personales, toda vez que dicha *atribución* es responsabilidad *de las instituciones de procuración de justicia e instituciones policiales* de los *tres órdenes de gobierno* y en el ámbito de sus respectivas competencias.

Otro de los puntos que fueron esenciales para la toma de decisiones por parte del entonces IFAI, fue delimitar y especificar en el estudio del caso, qué es la Plataforma México y de qué partes se compone, develando lo siguiente:

La Plataforma México es un conjunto de aplicaciones tecnológicas habilitadas en una red de telecomunicaciones, que permite la interconectividad entre diversos puntos del territorio mexicano y proporciona información sistematizada para la gestión policial, lo cual deriva en mayor apoyo logístico en el desempeño de las acciones en contra de la delincuencia y el crimen organizado, cuenta con mecanismos de seguridad, y resguardo de la información, para conservar la integridad de los datos, se integra por los siguientes sistemas de información y comunicaciones de alta tecnología al servicio de los cuerpos policiales y de las instancias de impartición de justicia del país:

- Informe Policial Homologado.
- Sistema de Gestión Operativa.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

- Cárdex Policial.
- SUIC.
- El Sistema Nacional de Información Penitenciaria.

Y, en lo concerniente al Registro Nacional del Personal de Seguridad Pública, contiene información de aspirantes y del personal activo de seguridad pública de los estados, el Distrito Federal (ahora Ciudad de México), los municipios y la Federación, además de los elementos de las empresas de seguridad privada. El registro consolida procedimientos de seguimiento y validación de información, y se ha tomado como base para la integración del Registro Nacional de Personal (Cárdex Policial).

G. *Resolución del pleno del Instituto Federal de Acceso a la Información Pública y Protección de Datos*

Se ordenó modificar la respuesta emitida por el Secretariado, y se le instruyó a dar respuesta en los siguientes términos:

- Emitir y poner a disposición del particular, previa acreditación de su personalidad, la resolución de su Comité de Información en la que fundara y motivara la improcedencia total o parcial de la corrección de datos personales.
- Indicar al recurrente, cuál fue la institución de seguridad pública que realizó el registro respectivo, a efecto de que pueda iniciar la solicitud de corrección, eliminación y/o cancelación de datos, según correspondiera (Informe, 2014).

En el siguiente apartado, retomaremos algunos aspectos relevantes que se dieron durante la sustanciación del recurso de protección de datos, y que justifican, desde mi punto de vista, la resolución del pleno del otrora IFAI, ahora INAI.

3. *Comentarios sobre el problema jurídico de fondo*

En el apartado anterior describimos los aspectos más relevantes relacionados con esta negativa del SESNSP hacia el particular, que deseaba conocer la información contenida en la Plataforma México, y así poder ejercer su derecho a conocer y rectificar sus datos, puesto que se veía

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

afectado en el ejercicio de otro u otros derechos, no sólo el laboral, sino también de los relacionados con la honra, su reputación y la continuación de su proyecto de vida profesional.

Lo que nos lleva a reflexionar respecto a si existía, en ese momento, congruencia normativa en lo concerniente al papel que desempeñaba el SESNSP, como operador y responsable de la información de los registros que forman parte de la Plataforma México, y que pudieran considerarse como datos personales sensibles. De tal manera que surge la interrogante sobre el posible problema o los problemas jurídicos de fondo:

¿Cuáles son los alcances de la publicidad de la información contenida en los registros de la Plataforma México?

En lo relativo al alcance de la publicidad, nos referiremos a ésta como la facultad de intercambio interinstitucional de los registros de las bases de datos que conforman la Plataforma México, y si bien es cierto, al que sólo tienen acceso las siguientes instituciones:

- Dependencias e instituciones de seguridad pública en los tres ámbitos de gobierno.
- Procuradurías generales de justicia federal y del fuero común (ahora fiscalías).
- Centros de reclusión federal, estatal y municipal.
- Centros de certificación, de acreditación y control de confianza.
- Consejos estatales de seguridad pública.
- Academias e institutos de seguridad pública y procuración de justicia.
- Dependencias e instituciones del Gobierno federal, que requieran permiso de acceso a las herramientas o aplicativos de la Plataforma.

También es cierto que la información fluye respecto del ámbito de competencia de cada una de éstas; y como se observó, en la revisión del caso de la persona quejosa, la institución de seguridad pública del Municipio de Juárez, en Nuevo León, tendría el dato del registro en Plataforma México, sin tener la información suficiente, por lo que dejó en duda o condición vulnerable su situación jurídica, en lo relativo a su conducta o desempeño como personal de seguridad pública.

Retomando la respuesta primigenia del SESNSP, éste aseguró no contar con atribuciones para corregir o cancelar la información de las bases de datos del Sistema Nacional de Información de Seguridad Pública, al referir que no operaba con datos personales del Registro Nacional de Personal de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Seguridad Pública, encontrándose imposibilitado jurídicamente para efectuar la corrección solicitada.

Sin embargo, en la respuesta a la solicitud de información adicional formulada por el comisionado ponente, contestaron que "conforme a lo dispuesto en el artículo 19 fracción I de la Ley General del Sistema Nacional de Seguridad Pública, la administración, de las bases de datos criminalística y de personal de seguridad pública, corresponde al Centro Nacional de Información".

Si reflexionamos respecto a las competencias del SESNSP, es el operador sin responsabilidad, más allá de guarda y custodia, y serán la Federación, los estados, la Ciudad de México (antes Distrito Federal) y los municipios, los responsables de suministrar, intercambiar, sistematizar, consultar, analizar y actualizar la información que diariamente se genere sobre seguridad pública; y de integrar y actualizar el SUIC con la información que generen las instituciones de procuración de justicia e instituciones de seguridad pública.

Aunque observamos falta de congruencia en sus respuestas, puesto que la administración de las bases de datos es tan amplia y ambigua que genera un margen de discrecionalidad no observado en las normas, según lo analizado hasta este punto, los datos personales que se niegan por el Secretariado en los registros son parte central de los mismos, por lo que se convierte en un asunto de mayor complejidad.

Veamos: la Plataforma México, en un sentido estricto, refiere principalmente al desarrollo de una red nacional que alberga las bases de datos de criminalística y de personal de seguridad pública, con el objeto de facilitar el suministro, actualización y consulta de los registros de las bases de datos de:

- Informe Policial Homologado.
- Registro Nacional de Información Penitenciaria.
- Registro de Licencias de Conducir.
- Registro Nacional de Armamento y Equipo.
- Vehículos Robados y Recuperados.
- Sistema Automatizado de Identificación Dactilar.
- Sistema Automatizado de Identificación de Voz.
- Sistema de Identificación de ADN.

De tal modo reiteramos que los registros en su mayoría se componen de datos personales que hacen identificables a las personas, incluso con datos biométricos como los de la voz, la identificación dactilar y de ADN.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Entonces, cuando el Secretariado indica que la información sobre elementos policiales o de seguridad pública contenida en la base de datos del Registro Nacional de Personal de Seguridad Pública, no es información concerniente a una persona física identificada o identificable, por lo que no constituye datos personales, éste se configura como un argumento débil, puesto que la calidad de los datos en el registro de nuestro interés tiene está naturaleza y se confirma en la respuesta al comisionado ponente con el numeral 1o.

Dada la naturaleza de la información de carácter confidencial, se considera que en su momento se vulneró el derecho a la protección de datos personales, sea el ejercicio de cualquiera de los derechos de acceso, rectificación, cancelación y oposición, por lo que debía ser procedente la cancelación u oposición al margen de publicidad (aunque interna), es decir, entre las instituciones autorizadas para el acceso a las bases de datos de la Plataforma México o interinstitucional; esta afirmación puede reforzarse con el análisis de la ponencia, cuando en su Informe de Labores del 2014 hace mención de la importancia de la resolución con casos similares en los expedientes de los recursos RPD/0578/14 y RPD/0580/14; así como el RPD/0579/14.

Por último punto, aunque en el orden de la resolución se indica como previo a lo anteriormente analizado, no deja de llamar la atención la omisión relativa a que el SESNSP no presentó ante el Comité de Transparencia la solicitud del particular, y cumplir con todas las formalidades del procedimiento establecido en la LFTAIPG y su Reglamento, y como resultado la falta de constancias de alguna manifestación de improcedencia de la corrección de datos personales, que hubiese sido facultad del Comité emitir, en una resolución fundada y motivada en que se determinara la improcedencia total o parcial de las correcciones solicitadas.

Esta práctica de decisión colegiada, mediante la intervención de diversas áreas que conforman la estructura del sujeto obligado, coadyuvan, sin duda, a la determinación de la clasificación de la información conforme a la normatividad de los sujetos obligados; lo que, a nuestra consideración, reduce el margen de error en el aseguramiento del resguardo o salvaguarda de la información o, en su caso, la garantía de acceso, sea en lo concerniente a la protección de los datos personales o la entrega de información pública.

La protección de los datos personales en el ámbito de seguridad pública no es un asunto simple, implica no sólo la afectación de las personas a las cuales no les benefició en su momento algún tipo de información con-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

tenida en la Plataforma México, y que tuvo repercusiones en sus derechos laborales o profesionales como el caso que se ha revisado en líneas anteriores, sino también se concatena con aspectos de bienestar de terceros.

III. Conclusiones

Es evidente que la realidad, en estos casos, supera a la norma; y esto es así, porque en el estudio de la resolución del IFAI nos enfrentamos, desde mi perspectiva, a una ponderación constante (aunque no especializada) de derechos, que ha resultado muy compleja. De inicio, si revisamos las bondades que ofrece la herramienta tecnológica, en este caso de la Plataforma México, estaremos convencidos de que a mayor información contenida en ella, mejores resultados tendrán los usuarios de la misma, que se reflejará directamente en las funciones de procuración de justicia, y de prevención o detección del delito en el caso de la seguridad pública; no obstante, se observa un incremento en el grado de discrecionalidad respecto a la acumulación y sistematización "justificada" de la información, sea estratégica o confidencial, en aras de cumplir con el objeto de la Ley General del Sistema Nacional de Seguridad Pública de regular la integración, organización y funcionamiento del Sistema Nacional de Seguridad Pública.

Sin embargo, como lo revisamos, la afectación a los derechos y libertades de las personas se ven vulnerados, si no se tiene el suficiente cuidado en su captura, manejo y "publicidad interinstitucional". En el caso concreto del particular con expediente RPD 0507/14, la acumulación de información en el espacio público fuera del contexto penal, le llevó a reclamar su derecho de cancelación debido a la falta de congruencia o claridad en la administración de los datos personales contenidos en los registros, y puso en evidencia que operó la falta de razonabilidad de las autoridades, al transmitir información privada de la cual no se tuvo, en su momento, la certeza de su verificabilidad o fiabilidad, o bien, que de manera automatizada se descarga sin un filtro humano que evite se generen estas afectaciones.

Con la resolución en comento, el pleno del IFAI le aseguró una vía para solicitar, de manera efectiva, la cancelación de sus datos personales, que tal vez por una homonimia le estaba afectando en su derecho fundamental a tener un empleo libremente elegido, y a sus derechos a la honra como servidor público en una institución policial, y a su propia reputación, manchada de forma indebida. El órgano garante del acceso la información

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

y la protección de datos personales, abrió un cauce al recurrente para la reparación de una iniquidad, y operó favorablemente para la restitución de sus derechos.

El uso de la tecnología, en materia de seguridad pública, es ya inevitable, y forma parte de nuestras vidas; pensemos ahora en la intervención de los registros de las llamadas o el acceso a una computadora de forma remota por medio del internet, incluso las cámaras de videovigilancia en la vía pública o en los hogares con las alarmas vecinales, los arcos lectores de placas, entre otras más. La acumulación de información sí incluye datos personales o patrimoniales que, en casi todos los casos, nos hacen identificables; y es por esto que, no sólo en México, ya se ha dado este debate sobre los límites y retos frente a los avances tecnológicos en el manejo de los datos personales, porque irremediablemente el uso de las tecnologías de la información conlleva a la responsabilidad de dar respuesta ante posibles amenazas a la violación de la privacidad.

Actualmente continuará siendo muy ardua la tarea del INAI en la revisión de casos relacionados con la seguridad pública, ya que se requiere proteger los derechos de las personas, sean de privacidad y/o de acceso a la información; y al mismo tiempo, permitir que su uso guarde proporcionalidad respecto del interés público de hacer pública la información o bien de la transmisión, que para efectos de este análisis denominamos publicidad interinstitucional de la información, y con esto se fortalezcan de manera justa los mecanismos y herramientas tecnológicas para combatir el crimen.

IV. Bibliografía

Aguilera Portales, Rafael Enrique y López Sánchez, Rogelio, 2007, "Los derechos fundamentales en la teoría jurídica garantista de Luigi Ferrajoli", *Revista Letras Jurídicas*, núm. 4, disponible en *https://archivos.juridicas.unam.mx/www/bjv/libros/6/2977/4.pdf*.

Ferrajoli, Luigi, 2001, "Derechos fundamentales", en Cabo, Antonio de y Pisarello, Gerardo (coords.), *Los fundamentos de los derechos fundamentales*, Madrid, Trotta.

Gallego García, Gloria M., 2004, "Sobre el monopolio legítimo de la violencia", *Revista de Derecho Penal*, Montevideo, Fundación de Cultura Universitaria, núm. 14.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

García Ramírez, Sergio, 2000, "En torno a la seguridad pública", en Peñaloza, Pedro José y Garza Salinas, Mario A. (coords.), *Los desafíos de la seguridad pública en México*, México, PGR-UNAM, Instituto de Investigaciones Jurídicas.

Instituto Federal de Acceso a la Información y Protección de Datos, 2015, *Informe de Labores 2014*, México, IFAI.

López Portillo Vargas, Ernesto y Barrena Nájera, Guadalupe, 2008, *Transparencia: ruta para la eficacia y legitimidad en la función policial*, México, IFAI, Cuadernos de Transparencia, núm. 14.

Mendoza Enríquez, Olivia A., 2018, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", *Revista IUS*, vol. 12, núm. 41, disponible en *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267&lng=es&tlng=es*.

Moreno Luce, Marta S., 2004, "La seguridad pública, los derechos humanos y su protección en el ámbito internacional", *Letras Jurídicas. Revista de los Investigadores del Instituto de Investigaciones Jurídicas de la U. V.*, núm. 9.

Ovalle Favela, José, 2016, "Derechos humanos y garantías constitucionales", *Boletín Mexicano de Derecho Comparado*, núm. 49, disponible en *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332016000200149&lng=es&tlng=es*.

1. *Legislación*

Cámara de Diputados, 2017, "Constitución Política de los Estados Unidos Mexicanos", *Diario Oficial de la Federación*, México, 15 de septiembre.

Cámara de Diputados, 2014, "Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental", *Diario Oficial de la Federación*, México, 14 de julio.

Poder Ejecutivo Federal, 2009, "Ley General del Sistema Nacional de Seguridad Pública", *Diario Oficial de la Federación*, México, 2 de enero.

Poder Ejecutivo Federal, 1988, "Ley General del Equilibrio Ecológico y la Protección al Ambiente", *Diario Oficial de la Federación*, México, 28 de enero, disponible en *https://www.dof.gob.mx/nota_detalle.php?codigo=4718573&fecha=28/01/1988*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

2. *Sitios web*

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, disponible en *http://inicio.ifai.org.mx/SitePages/ifai.aspx*, consultada el 29 de octubre de 2018.

México Evalúa, 2018, "México Evalúa. Datos para debatir seguridad pública", 23 de abril, disponible en *https://www.mexicoevalua.org/2018/04/23/datos-debatir-seguridad-publica/*, consultada el 2 de noviembre de 2018.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

Reseñas bibliográficas

Universidad Nacional Autónoma de México, IIJ-BJV, 2020
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

DICCIONARIO DE PROTECCIÓN DE DATOS PERSONALES

*Isabel Davara Fernández de Marcos**

El *Diccionario de protección de datos personales. Conceptos fundamentales*, editado por el Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI) en noviembre de 2019, y presentado de forma oficial en febrero de 2020, es una obra que se caracteriza por su carácter inédito y un alto grado de detalle, reflejado en el estudio de cada uno de los conceptos que lo conforman. Actualmente, es el primer "diccionario de conceptos" (más que de definición de voces) que existe en la materia de protección de datos personales. En cada una de sus voces se siguió una serie de pautas editoriales para garantizar la coherencia, alcance y calidad del contenido de la obra.

Antes de continuar con esta reseña, no puedo sino manifestar mi profundo agradecimiento al INAI por la confianza depositada en mí para coordinar y coescribir esta ambiciosa obra.

De la consulta del *Diccionario*, ya sea en su versión electrónica o impresa, se advierte, con lujo de facilidad, que más que un tradicional repositorio de términos es un libro que reúne, bajo muy específicos criterios de investigación y de edición jurídicos, el estudio de los conceptos elementales de la materia que nos ocupa. El *Diccionario* en cuestión es una obra única en su género, no sólo en México, sino internacionalmente. A la fecha, no conocemos en el mundo, por su alcance y estructura, un documento similar.

* Licenciada y doctora en derecho, y en ciencias económicas y empresariales, por la Universidad Pontificia Comillas de Madrid. Abogada practicante en México y en España. Socia fundadora del despacho Davara Abogados, firma legal especializada en Derecho digital, tecnología e innovación. Coordinadora y profesora en Posgrado en el ITAM. *idavara@davara.com.mx*.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

La elaboración del *Diccionario* tuvo como fundamento un sólido proceso de coordinación y asistencia editorial para cada uno de los magníficos y excepcionales autores con los que se contó. Aunque en un primer momento se podría haber pensado en sólo aglutinar una serie de términos legales, la realidad de la práctica cotidiana y la necesidad de contar con una obra dogmática, pragmática y de contenido jurídico vigente, con una estructura profunda y detallada, dio el impulso necesario para estudiar, con un considerable nivel de detalle, cada institución jurídica relacionada con el derecho de protección de datos personales.

En este orden de ideas, para comprender el resultado final, es esencial distinguir varias etapas en la confección de esta obra.

En primer lugar, se llevó a cabo un proceso de análisis teórico para elegir los términos fundamentales en esta materia, de suerte que en este *Diccionario* el lector podrá localizar conceptos que no podrían faltar, como datos personales, derechos ARCO, protección de datos personales, autodeterminación informativa, privacidad, vida privada y organismos garantes, por mencionar algunos. Pero también se encuentran muchos otros que, no siendo tan frecuentes —al menos en las leyes de protección de datos personales—, resultan de gran relevancia para entender el derecho en su conjunto, y la actualidad del mismo, como *big data*, monetización de datos, inteligencia artificial, aprendizaje de máquinas y muchos otros.

En segundo lugar, se establecieron las directrices editoriales para la creación de cada definición y se generaron materiales de orientación para los autores (tablas analíticas sobre la recepción legal, jurisprudencial y de organismos internacionales relevantes de cada término, a nivel nacional e internacional) con el objeto de procurar la cohesión y neutralidad en la redacción de cada voz.

Finalmente, la última etapa de este proceso de preparación fue la revisión exhaustiva de cada elemento que integra el *Diccionario*, con el fin de asegurar la calidad y homogeneidad del contenido, para así enviar estas directrices a cada autor, previamente seleccionados de manera cuidadosa por su experiencia y conocimiento: como queda absolutamente claro, al leer los grandes nombres y referencias doctrinales que han hecho el honor de acompañarnos.

De la explicación que antecede, el lector podrá concluir que la aproximación a cada voz buscó cumplir con altos estándares de calidad y objetividad en la explicación de los términos. Uno de los principios rectores, al aproximarnos a cada uno de ellos, ha sido recoger, en la medida de lo posible, todas aquellas fuentes legales y normativas que nutren el contenido de cada voz, cuando así ocurre: de manera que el lector pueda encontrar

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

un compendio de las referencias ahí establecidas, y así poder contar con una visión lo más comprehensiva posible de cada una de las voces, involucrando aspectos conceptuales y normativos a nivel nacional y a nivel internacional cuando era conveniente.

En este punto, no puedo omitir agradecer ampliamente al personal del INAI por haber colaborado, inmensurablemente, en la edición de esta obra, situación que sabemos no ha sido una tarea sencilla, considerando las magnas características de la tarea.

La obra abarca el análisis de las dos esferas regulatorias existentes en México. Es decir, la regulación presente en el sector público y aquella perteneciente al sector privado, así como las principales tendencias internacionales. De esta suerte, el lector podrá advertir que se ha tenido la intención de que cada definición incluya un sustento normativo, jurisprudencial y dogmático, de acuerdo con las previsiones legales y experiencia práctica surgida a partir de la aplicación del derecho de protección de datos personales en los referidos sectores de actividad.

El *Diccionario* consta de 898 páginas, donde se incluyen 206 definiciones que, en promedio, tienen una extensión de 6 cuartillas. Sin embargo, en algunos casos muy concretos, por la complejidad e importancia de la voz estudiada se amplió la explicación a un mayor número de páginas. Por ejemplo, las voces de derecho al honor, derecho a la intimidad y vida privada requirieron un amplio detalle explicativo, dada la amplitud de criterios existentes y su regulación vigente.

Como decía, en el *Diccionario* se encuentran las definiciones básicas previstas en la normatividad, como aviso de privacidad, bases de datos, bloqueo, dato personal, datos personales sensibles, deberes de protección de datos (seguridad y confidencialidad), consentimiento, derechos ARCO, derecho al olvido, disociación, responsable, encargado, titular, tercero, fuente de acceso público, tratamiento, tratamiento intensivo, principios de protección de datos personales (licitud, lealtad, información, consentimiento, calidad, finalidad, proporcionalidad y responsabilidad), remisión, transferencia, entre otras. Cada definición incluye, cuando es requerida, la comparación entre la regulación del sector público y la del sector privado; y en su caso, referencias a la normatividad internacional, si es conveniente.

El *Diccionario* también incluye conceptos procesales relacionados con la aplicación de la normatividad en los sectores público y privado, ya que tanto la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados regulan aspectos adjetivos referentes a los distintos procedimientos administrativos, que se sustancian

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

ante el INAI y los respectivos organismos garantes locales, como requerimiento, procedimiento de investigación, investigaciones previas, procedimiento de verificación, procedimiento de imposición de sanciones, juicio contencioso administrativo federal, juicio de amparo, entre otros.

Asimismo, en este *Diccionario* se agregan conceptos novedosos que reflejan el constante y acelerado desarrollo tecnológico al que nos encontramos expuestos. Hablamos de definiciones actuales como anonimización, seudonimización, aprendizaje de máquinas, *big data, cookies, web beacons*, inteligencia artificial, internet de las cosas, monetización de datos, entre otras. El derecho a la protección de datos personales es una materia viva, y esperamos que la incorporación de estas voces ayude a sus lectores a comprender las profundas implicaciones que tienen los nuevos desarrollos tecnológicos en el ámbito del derecho a la protección de datos personales.

Finalmente, con relación al ámbito internacional, además de las posibles comparaciones cuando los términos lo requieren, el *Diccionario* también analiza conceptos relevantes en dicho entorno, que usamos con mucha cotidianeidad, como Reglamento General de Protección de Datos Personales, Convenio 108, Estándares de Protección de Datos para los Estados Iberoamericanos, Directrices de Privacidad de la OCDE, Sistema de Privacidad APEC, Sistema de Protección de Datos en Estados Unidos de América, Declaración de Madrid, entre otras.

Este trabajo ha sido cobijado por la experiencia y profesionalismo de treinta y cinco grandes especialistas nacionales de reconocido prestigio de diversas instituciones, comprendiendo tanto centros de estudio e instituciones académicas reconocidas, como instituciones de impartición de justicia, instituciones privadas y órganos consultivos. Resaltar sólo alguno de ellos sería imposible, porque su prestigio académico y profesional habla por sí mismo. Ha sido un gran honor contar con el apoyo de tan connotados autores especialistas, y cuya participación garantiza la calidad y valía de esta obra. Me siento profundamente conmovida por su generosidad intelectual y humana.

Dado que el derecho, en general, y el novedoso derecho de protección de datos personales, en particular, tienen un carácter dinámico, uno de los principales retos, además de la mera consecución de esta monumental empresa, es mantener la obra al día y contar con referencias actuales que sirvan para que las personas interesadas en conocer la materia de protección de datos personales puedan entender las implicaciones legales y prácticas de los términos que conforman el *Diccionario*.

Asimismo, considerando que en México y en el mundo estamos construyendo día a día este derecho a la protección de datos personales, que

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

cada día muestra más aristas y consecuencias desconocidas, en cantidad y en profundidad, aún tenemos mucho camino por recorrer. Además, no podemos descartar la posibilidad de que el marco jurídico actual sea reformado, y en consecuencia nuestras definiciones deban serlo también. Por ejemplo, en el último año hemos sido testigos de una copiosa cantidad de iniciativas para reformar la LFPDPPP, en temáticas como derecho al olvido, portabilidad, consentimiento, notificación de vulneraciones de seguridad, entre otras.

Somos conscientes de que hay y habrá espacio para muchas mejoras en el tiempo, pero consideramos que el esfuerzo y la dedicación de los autores lograron que esta obra sea, con un importante nivel de detalle, un excelente punto de partida para toda persona que requiere contar con referencias precisas sobre las principales instituciones del derecho a la protección de datos personales en México, a la par que representa el panorama regulatorio de este derecho en nuestro país.

De esta manera, los ensayos que conforman este *Diccionario* cumplen un doble propósito: fungen como un instrumento de difusión de la cultura de protección de datos personales y sirven como un mecanismo habilitante para el ejercicio del derecho a la protección de datos personales, pues la información ahí contenida tiene el potencial de empoderar a las personas titulares de dichos datos para tomar decisiones conscientes sobre el uso de sus datos personales, y con esto coadyuvar a la garantía del derecho a la protección de datos personales.

Reitero mi más profundo agradecimiento al INAI, por el encargo de liderar esta magna tarea; a los autores, por su indispensable y excepcional contribución para el éxito de la misma; y a mi equipo más cercano —en especial a los maestros Gregorio Barco Vega y Alexis Cervantes Padilla—, sin el cual esta empresa no habría sido posible. Espero que la obra satisfaga las más altas expectativas y cumpla el propósito de fomentar y fortalecer la cultura de la protección de datos personales en México y en la región.

Bibliografía del libro reseñado

Fernández de Marcos, Isabel Davara (coord.), *Diccionario de protección de datos personales. Conceptos fundamentales*, México, INAI, 2019.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

NORMAS DE PUBLICACIÓN

La revista académica *Estudios en Derecho a la Información* es una publicación semestral que editan el Instituto de Investigaciones Jurídicas de la UNAM, la Facultad de Ciencias Políticas y Sociales de la UNAM, el Instituto Nacional de Transparencia, de Acceso a la Información y Protección de Datos Personales (INAI), y el Centro de Investigación y Docencia Económicas (CIDE). La revista publica manuscritos cuyo eje temático sea el derecho a la información, a través de estudios caracterizados por ser multidisciplinarios y plantear cuestiones sobre el papel de las normas jurídicas y las políticas públicas en los procesos de desarrollo institucional, impacto económico, comunicación, gobierno y poder.

Se reciben exclusivamente trabajos originales y que no hayan sido publicados con anterioridad. Los manuscritos son considerados para su publicación preferentemente cuando emplean técnicas de investigación empírica, datos estadísticos, análisis cualitativo y/o cuantitativo en un estilo crítico y analítico, incluyendo hipótesis, argumentación, contraargumentación y notas concluyentes.

Los manuscritos recibidos deben aportar una contribución académica sustancial en los temas que incluye esta revista dentro del derecho a la información: derecho de acceso a la información pública, transparencia gubernamental y rendición de cuentas; protección de datos personales y privacidad; tecnologías de la información y de la comunicación; libertad de expresión y periodismo; regulación y políticas de los medios de comunicación y telecomunicaciones.

Los artículos y comentarios jurídicos sometidos a consideración de la revista deben incluir un resumen de no más de 250 palabras, y de 3 a 5 palabras clave que reflejen el contenido del manuscrito. Los textos deben estar divididos en secciones, incluyendo la bibliografía o referencias utilizadas. Las notas a pie de página se deben incluir en caso de que sean estrictamente necesarias y con contenido sucinto. Se evitará subrayar o resaltar en mayúsculas y negritas el texto; el uso de itálicas se reserva para los términos en otro idioma, los títulos de publicaciones u obras, y las li-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2021.11.15305

gas de fuentes en internet. Se evitarán las citas textuales mayores a las 40 palabras, excepto en los comentarios jurídicos cuando sea estrictamente necesario.

Los artículos no deben exceder las 20 páginas a interlineado 1.5, incluyendo tablas y gráficas; los comentarios jurídicos tendrán una extensión de hasta 15 páginas a interlineado 1.5. Las reseñas de libros no deben rebasar las 10 páginas. La letra estándar para manuscritos es Arial, 12 puntos. Se reciben manuscritos en español, inglés, portugués, italiano o francés. La revista publica textos que utilicen el sistema de citación del Instituto de Investigaciones Jurídicas de la UNAM, de acuerdo con sus *Criterios editoriales*, exclusivamente en el Sistema Harvard.

La revista se reserva el derecho de mejorar los manuscritos como parte del proceso editorial, aclarando la redacción o corrigiendo faltas ortográficas y/o gramaticales.

Los artículos, así como los comentarios jurídicos que sean preseleccionados por el Comité Editorial, pasarán al proceso de dictaminación o arbitraje doble ciego. Los dictámenes pueden determinar que los manuscritos son publicables, no publicables o condicionados a cambios.

Recepción de manuscritos

La recepción de manuscritos es únicamente por la página web de la revista a través de su "Usuario" (*https://revistas.juridicas.unam.mx/index.php/derecho-informacion*). Si no tiene "Usuario", debe crearlo en "Registro de usuarios", que se encuentra en "Información para autores" (es importante que se complete el formulario de registro con el mayor número de datos requeridos, y el nombre de usuario tendrá que estar en el siguiente formato: "Nombre_Apellido"). Al ingresar al sitio con su "Usuario", debe dar clic en "nuevo envío", seguir las instrucciones para llenar el formulario y adjuntar su manuscrito (al "subir archivo" seleccione la ubicación de su documento dentro de su computadora y, posteriormente, dé clic en "Cargar"). Para mayor información y dudas deberá mandar un correo a *redi.iij@unam.mx*.

Revista Estudios en Derecho a la Información, núm. 11, editado por el Instituto de Investigaciones Jurídicas de la UNAM, se publicó en versión digital el 10 de diciembre de 2020. En su composición tipográfica se utilizó tipo *Fairfield LT Std* en 9, 10 y 11 puntos.