PRIVACIDAD VS PUBLICIDAD DE LOS DATOS PERSONALES EN POSESIÓN DE AUTORIDADES.

Autor: Dulcemaría Martínez Ruíz

Referencia Institucional: Fondo de Información y Documentación para la Industria de México.

Mail: dulcema21@hotmail.com

dmartinezr@cinepolis.com

Resumen

Palabras clave: datos personales, particulares, autoridad, privacidad, publicidad.

PRIVACIDAD VS PUBLICIDAD DE LOS DATOS PERSONALES EN POSESIÓN DE AUTORIDADES.

INTRODUCCIÓN

La protección de los datos personales es una obligación a cargo de los particulares y de las autoridades, dentro de la cual, tienen que velar por el cumplimiento de los principios tales como la privacidad y la confidencialidad de la información, así como de el establecimiento de una serie de medidas seguridad y de control que permitan la salvaguarda, protección, privacidad y confidencialidad de dichos datos mientras los mismos se encuentren sujetos al tratamiento de los entes públicos y/o los privados.

Dependiendo de la legislación que se trate, existe la posibilidad de que la protección de los datos personales en posesión de los particulares u organismos públicos se encuentren regulados por la misma legislación y/o en legislaciones separadas, como lo es el caso de México, sin embargo, lo importante es que la o las legislaciones que contengan dicha protección establezcan las obligaciones, requisitos y medidas de seguridad a cargo de las autoridades y/o de los particulares.

Ahora bien, con la apertura y el desarrollo del gobierno electrónico, tanto México como otros países han venido implementando programas, plataformas y sistemas electrónicos que permiten a la ciudadanía el tener accesos mucho más fáciles a las bases de datos o registros públicos que contienen información y datos personales de la ciudadanía, tales como registros públicos de actas de nacimiento, de defunción o de matrimonio; o registros públicos de inmuebles, de seguridad social o incluso de profesiones.

Lo anterior, si bien es cierto representa una serie de avances relacionados con la aplicación de las nuevas tecnologías de información y comunicaciones en beneficio de la ciudadanía, también puede convertirse en un factor de riesgo para la misma, ya que en muchas de las ocasiones, por la facilidad y rapidez en la localización de la información y datos personales de una persona, las mismas pueden constituir una herramienta de gran utilidad para quienes realizan minería de datos o incluso, puede llegar a trascender incluso al hecho de que funcionen como una herramienta para suplantar la identidad de una persona y/o para cometer actos de extorsión, amenazas o delincuencia organizada.

La minería de datos antes mencionada, no solamente puede ser realizada a través de bases de datos o fuentes de acceso público instaladas en plataformas o medios electrónicos, sino que incluso, puede realizarse de manera personal, cuando realizamos consultas de información de manera directa en los registros públicos que correspondan.

Es decir, en el caso de los datos personales en posesión de las autoridades, nos encontramos con una doble dualidad en el manejo de la información ya que, por una parte, las autoridades tienen la obligación de garantizar la privacidad, resguardo confidencialidad de los datos personales contenidos en sus bases de datos, sin embargo, cuando dichos datos personales se encuentran en documentos o constancias que forman parte de los registros públicos, dichos documentos y los datos personales en ellos contenidos, tienen que ser públicos y de fácil acceso a la ciudadanía.

Ahora bien y ejemplificando lo anterior de manera tal vez muy radical, podríamos decir que un mismo dato personal deberá ser guardado y protegido por una autoridad cuando el mismo no

conste en un documento o base de datos que forme parte de una fuente de acceso públicos, ya que en el momento en el que el mismo dato personal pasa a una fuente de acceso público, entonces deberá ser público y accesible a toda la ciudadanía, sin que exista entonces para su consulta algún tipo de control o medida de seguridad que proteja los datos personales.

Lo anterior no significa que los datos contenidos en los registros públicos o fuentes de acceso públicos no estén siendo tratadas de manera correcta o sin contar con las facultades necesarias para otorgar y facilitar la publicidad de la información, sin embargo, dados los cambios de cultura que estamos viviendo y sobre todo, con el incremento en algunos riesgos, tales como el incremento en la inseguridad que hemos estado viviendo en los últimos años en algunos países latinoamericanos, ha llegado el momento de replantearnos la posibilidad o incluso la necesidad de establecer medios de control que permitan el garantizar la protección de los ciudadanos sin que ello implique el restringir las funciones o finalidades de los registros públicos.

DATOS PERSONALES

Para comenzar con el presente análisis, es importante establecer y definir que se entiende como dato personal, es importante mencionar que tanto las Directrices que rigen la Protección de la Intimidad y de la Circulación Transfronteriza de los Datos Personales, como el Convenio No. 108 del Consejo de la Comunidad de Europa y el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico los definen como "*Cualquier información relativa a una persona física identificada o identificable*"[1]. Así mismo y de una manera un poco más amplia, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, define a los datos personales como "*toda información sobre una persona física idientificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*".[2]

La legislación mexicana, retomando las definiciones antes señaladas, define como dato personal a "*Cualquier información concerniente a una persona física identificada o identificable*"[3],

concepto que para el objeto del presente estudio es aplicable tanto a los datos personales que se encuentren en posesión de las autoridades y de los particulares.

En México, la protección de los datos personales se encuentra regulada en legislaciones diferentes, ello dependiendo de si los mismos se encuentran en posesión de entes públicos o privados; de manera que, los entes públicos son regulados por las legislaciones que garantizan la transparencia y el acceso a la información gubernamental, tal y como es el caso de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Ley de Transparencia), la cual, tiene "la finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal,"[4] mientras que los datos personales en posesión de los particulares se encuentran regulados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley de Datos), cuyo objeto es "la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas."[5]

Ahora bien, lo importante es que ambas legislaciones establecen la obligación a cargo de los entes públicos o privados de respetar los principios del tratamiento de los datos personales, así como el deber de respetar una serie de medidas de seguridad y de control que permitan la protección y resguardo de los datos personales de los particulares.

Privacidad

En primer lugar, vale la pena definir que se entiende como privacidad, para lo cual cito la definición establecida por la Real Academia de la Lengua Española, ya que establece que privacidad es el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión"[6], es decir, que como ciudadanos y titulares de nuestros datos personales tenemos derecho a proteger ciertos datos e información dentro de nuestra esfera más intima de protección o en el caso de que decidamos otorgar el permiso o facultad a otra persona, sea particular o

autoridad, para que realice el tratamiento de nuestros datos, dicho individuo o autoridad tiene que garantizar la protección y privacidad de nuestros datos personales, es decir, de su privacidad.

Ahora bien y encuadrando la definición de privacidad con lo establecido en la legislación mexicana, en la misma se ha establecido que para el tratamiento de los datos personales en posesión de los particulares, se presume que existe la expectativa razonable de privacidad, por medio de la cual, el titular de los datos personales deposita su confianza en otra persona para que pueda llevar a cabo el tratamiento de sus datos personales conforme a los términos establecidos en la ley[7].

Así mismo y en relación a los datos personales regulados por las autoridades, el principio de privacidad lo encontramos dentro del principio de confidencialidad, ya que se establece que las autoridades o sujetos obligados "…no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información".[8]

Con el creciente incremento en el uso de los medios de comunicación, con la digitalización de plataformas y bases de datos que contienen datos personales, así como con el fácil y rápido flujo de datos personales a nivel nacional e incluso internacional, el tema de la privacidad cobra un aspecto muy importante a vigilar, ya que la misma puede ser vulnerada en cualquier momento y de una manera mucho más rápida mediante el uso de las tecnologías de la información y comunicaciones.

Las vulneraciones a la privacidad o incluso el mal uso de la información contenida en las fuentes de acceso público, cobra importancia sobre todo cuando vemos el daño o la extracción de información en su conjunto y no como un dato aislado, es decir, "la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a permanecer reservado."[9]

Cuando nuestros datos personales se encuentran dispersos y disponibles en fuentes de acceso público que contienen datos o información aislada no representan mayor problema, sin embargo, cuando se realiza por ejemplo minería de datos en las diversas fuentes de acceso público, se pueden llegar a construir perfiles muy complejos y completos que contendrán información de las personas, lo cual, podría llegar a ser utilizado para violentar o transgredir el derecho a la privacidad de los datos personales de cualquiera de los titulares de la información, e incluso, yendo más allá, los perfiles obtenidos pueden llegar a ser utilizados para cometer ilícitos en contra de su titular, tales como la suplantación de identidad.

TRANSPARENCIA Y FUENTES DE ACCESO PÚBLICO

Transparencia

Antes de entrar al análisis de los datos personales que se encuentran establecidos en las fuentes de acceso público o en propiedad de las autoridades, considero importante definir el concepto de transparencia y con ello, marcar la diferencia entre ambos conceptos.

La palabra transparencia deriva del latín *trans* (mas allá o a través de) y de *parere* (aparecer, mostrar o mostrarse), así mismo, conforme a la legislación mexicana, la Ley de Transparencia establece la obligación de que las dependencias e instituciones públicas (sujetos obligados) deban poner a disposición del público y mantener actualizada cierta información, entre la que destaca la relacionada con su estructura orgánica, con las facultades de sus unidades administrativas, el directorio de los servidores públicos, la remuneración mensual de sus servidores públicos[10], entre otra información que tales dependencias tienen la obligación de transparentar y publicitar, es decir, esta información debe ser puesta a disposición de manera oficiosa, sin que medie solicitud por parte de algún ciudadano.

Además de dicha información publicada de manera oficiosa, los sujetos obligados o autoridades tienen la obligación de atender y resolver solicitudes de acceso a la información que les realicen

los particulares, la cual puede tratarse de información contenida o no dentro de la información publicada de manera oficiosa.

Para esclarecer el concepto de transparencia, es importante establecer la diferencia entre el concepto de transparencia y el de publicidad de la información, ya que el mismo es mucho más amplio que el segundo, en el sentido de que "…la publicidad implica mostrar, pero la transparencia implica algo más que mostrar, implica dejar ver, simplemente que el actuar de la administración pública se deje ver como a través de un cristal."[11]

Ahora bien, es importante establecer que no toda la información contenida en las bases de datos o archivos de las autoridades se encuentra sujeta a la transparencia, sino que existe cierta información que será tratada como información reservada o confidencial.

Conforme a la legislación mexicana, encontramos que los datos personales que requieren el consentimiento de los individuos para su difusión, distribución o comercialización en términos de lo establecido en la legislación de transparencia, se consideran datos sujetos a la confidencialidad de las autoridades y por ello no podrán ser divulgados por las mismas.

Sin embargo, lo anterior a su vez tiene otra excepción, ya que no se consideraran confidenciales los datos personales o la información que se encuentre en los registros públicos o en las fuentes de acceso público.[12]

Fuentes de acceso público

Conforme al Marco de Privacidad del Foro de Cooperación Económica Asía Pacífico, encontramos que la información a disposición del público es la información personal acerca de un individuo, que él mismo hace o permite que esté disponible al público, o es obtenida o accedida legalmente desde registros del gobierno que están disponibles para el público.[13]

Así mismo y como se definió con anterioridad, en materia de transparencia se establece como excepción al principio de confidencialidad de los datos personales, los datos personales o

información que se encuentre contenida en los registros públicos o en las fuentes de acceso público, con lo cual, se legitima la función y finalidad de dichos registros públicos, es decir, se garantiza la publicidad oficial de la situación jurídica de los actos contenidos en los mencionados registros.

Para mayor entendimiento de lo anterior, otro ejemplo del respeto a la naturaleza y principios de publicidad de los actos contenidos en los registros públicos, la misma excepción se estipula en la Ley de Datos Personales, ya que establece que no será necesario el consentimiento para el tratamiento de los datos personales en posesión de los particulares, cuando los datos figuren en fuentes de acceso público.[14]

La legitimación de lo anterior, garantiza una convivencia armónica y equilibrada entre transparencia y privacidad, ya que no se ni se realiza una publicidad total de los datos ni se realiza una restricción total la información y datos personales contenidos en las bases de datos o registros públicos.

GOBIERNO ELECTRÓNICO

Gracias al creciente uso de las Tecnologías de la Información y Comunicaciones (TIC), los gobiernos han ido transformando o migrando la gestión y administración pública de cierta información, trámites o servicios a través de las plataformas y elementos brindados por dichas tecnologías.

Es decir, las TIC se han convertido en una "…herramienta para mejorar la atención ciudadana, los trámites y servicios, la posibilidad de gobernar en la red y de ser un instrumento que promueva la democracia y los valores democráticos en las sociedades".[15]

Dentro de las herramientas instrumentadas tanto en México como en otros países se encuentran por ejemplo, el montar y poner a disposición del público en plataformas electrónicas la información y documentos de los registros públicos, la cual, si bien es cierto y conforme a lo

expuesto con anterioridad, constituye parte de la información pública que no se encuentra sujeta a confidencialidad en materia de transparencia y de protección de datos, si se han convertido en mecanismos mediante los cuales cualquier ciudadano puede obtener información hasta construir el perfil personal de cualquier persona.

Ejemplo de lo anterior, fue el caso ocurrido en el año 2012 en la ciudad de Morelia, Michoacán, México, por el cual y presumiblemente con la finalidad de facilitar el acceso a la ciudadanía de cierta información, la Dirección del Registro Civil del Estado de Michoacán publicó en su página web la base de datos de todas las actas de nacimiento de los ciudadanos nacidos en el estado de Michoacán, mediante la cual, con el simple hecho de ingresar el nombre de cualquier persona y su fecha de nacimiento, podías ingresar y descargar el acta de nacimiento de cualquier ciudadano michoacano[16].

En un estado o país en donde reine la seguridad total, podríamos pensar que se trata de un eficiente uso de las tecnologías de la información con la finalidad de poner la información a disposición de la ciudadanía y que ello no implicaría ningún riesgo, sin embargo, la información contenida en los registros públicos también podría ser utilizada con fines ilícitos, los cuales en muchas ocasiones derivarán de la construcción de perfiles.

Construcción de perfiles derivada de fuentes de acceso público

Tomando el ejemplo de México y de manera muy general, podemos especificar que extrayendo información de los registros públicos o de las fuentes de acceso público, cualquier persona puede llegar a obtener la siguiente información de cualquier persona, ello sin dejar un solo dato, registro o indicio que refiera o permita identificar a la persona que realiza la búsqueda de información:

1. Nombre, apellido, nacionalidad, fecha de nacimiento, edad, nombre y apellido de los padres y estado civil. Información que puede ser extraída de las actas de nacimiento, defunción o matrimonio, las cuales y dependiendo de la plataforma utilizada por la autoridad responsable, pueden ser consultadas a través de sitios web o cajeros automáticos, los cuales de la misma forma que las páginas web, con el solo dato del

nombre y fecha de nacimiento, defunción o matrimonio, puedes obtener el acta que corresponda.

2. Número de Clave Única del Registro de Población (CURP). Número que puede ser obtenido vía web.[17]

3. Número de cédula, profesión o carrera concluida, año de expedición de la cédula, universidad en la que se estudió. Lo anterior se obtiene en el Registro Nacional de Profesionistas de la Secretaría de Educación Pública vía web.[18]

4. Número de seguridad social y nombre del patrón (NSS).[19]

5. Monto ahorrado para adquirir un crédito inmobiliario ante el Instituto del Fondo Nacional de Vivienda para los Trabajadores (INFONAVIT).[20]

6. Número de Registro Federal de Contribuyentes (RFC). Al realizar la consulta del monto ahorrado para adquirir un crédito inmobiliario, el resultado de la búsqueda también arroja el RFC.

7. Información de bienes inmuebles. Si bien la base de datos y registro público de inmuebles no se encuentra disponible en alguna página web, en algunos Estados existen computadoras o equipos que permiten realizar las búsquedas de los bienes inmuebles que corresponden a cualquier persona.

Conforme a los puntos antes enunciados, resulta paradójico que el poner a disposición de los particulares las herramientas de consulta y de obtención de documentos contenidos en los registros públicos, es el hecho de que cualquier persona pueda tener acceso a tus datos personales e incluso construir un perfil muy amplio de tu situación personal, laboral y económica de cualquiera de nosotros, ello con el simple hecho de consultar dichas las fuentes y bases de datos de acceso público de muchas dependencias u organizaciones públicas.

Riesgos

Los anteriores, son los principales datos que pueden ser extraídos de las bases de datos o registros públicos, los cuales y como se mencionó con anterioridad, al ser obtenidos o tratados por un tercero de manera individual no representarían un gran riesgo, sin embargo, al ser compilados y asociados a una sola persona o identidad puede implicar graves riesgos a la seguridad de las personas.

Riesgos entre los cuales, destaca robo o usurpación de identidad, acto mediante el cual una persona se hace pasar por otra con la finalidad de realizar trámites u obtener beneficios económicos en su nombre, tales como créditos o acceso a su información financiera, o en su caso, también puede ser realizado con las finalidades de cometer ilícitos refugiándose en identidades falsas y/o con la intensión de perjudicar al titular de los datos personales, ello mediante difamación o mediante actos que pongan mal su nombre e identidad.[21]

Tal es la importancia y fuerza que ha cobrado la suplantación de identidad, que al 30 de septiembre del 2013, se reportó que México ocupa el tercer lugar en robo de identidad en América Latina, mientras que el primero y segundo lugar los ocupan Colombia y Brasil, respectivamente. El robo de identidad relacionado con estos países en mucho tiene que ver con el uso de documentos oficiales que realizan ciertas personas para obtener créditos o acceso a información financiera de los titulares de los documentos utilizados, documentos oficiales que en el caso de México, son muy fáciles de conseguir por cualquier persona, tal y como es el caso del acta de nacimiento, ya que la misma puede ser adquirida por ejemplo en alguno de los cajeros automáticos de actas de nacimiento, en donde, únicamente se tiene que ingresar el pago, el nombre de la persona y su fecha de nacimiento.

Así mismo, la construcción de perfiles derivados de las bases de daros o registros públicos y dada la situación de seguridad existente en algunos países, puede servir a los delincuentes para cometer delitos de amenazas o extorción.

Lo anterior ya que en un momento de vulnerabilidad y presión psicológica, los delincuentes pueden proporcionar a la victima información relacionada con su familia, tales como nombres de los padres (obtenidos del acta de nacimiento), mencionar que conocen los inmuebles que posee (obtenidos de los registros públicos de la propiedad raíz) o incluso, mencionar que saben donde trabaja o tienen su expediente laboral (obtenidos de la información contenida en las bases de datos del INFONAVIT), lo anterior a su vez, podría derivar en delitos más serios y peligrosos tales como el secuestro.

Mejores prácticas

El garantizar la publicidad y fácil acceso a los registros públicos, y a su vez, el vigilar y proteger la privacidad y el uso adecuado de los datos personales e información en ellos contenidos, representa uno de los retos más importantes de los países, ello ya que tienen que buscar el adecuado equilibro entre una y otra practica.

Por lo anterior, es conveniente citar algunas de las mejores prácticas utilizadas por algunos países, mediante las cuales, se implementan mayores puntos de control o identificación que permitan a las personas acceder a la información contenida en los registros públicos de una manera más segura o controlada:[22]

1. En Perú, se implementó el Servicio de Verificación Biométrica con el Colegio de Notarios de Lima.[23]

   Servicio que tuvo como antecedente la inseguridad jurídica que pasaban los ciudadanos sobre todo al momento de realizar operaciones tales como la compra o venta de inmuebles, y por lo tanto, los notarios no tenían la forma de identificar o frenar la suplantación de edad.

   Por ello se implementó dicho servicio, mediante el cual se permite la identificación en línea de las personas que acuden ante las entidades públicas o privadas a realizar algún trámite. Esto mediante la identificación biométrica, que permite a las instituciones

públicas o privadas la suplantación de identidad y evitar fraudes mediante la correcta autenticación de las personas.

Algunos de los beneficios obtenidos con este Servicio son:

- El minimizar la suplantación y estafa de personas.
- Se estableció una medida de seguridad y control en el acceso a la prestación de los servicios.
- Se puede aplicar a diversos sectores tanto públicos como privados, siempre y cuando requieran la validación de la identidad de las personas para poder realizar o efectuar sus trámites.
- Es de fácil utilización e incorporación a los sistemas de los clientes finales.

2. En Ecuador, se implementó el Proceso de Magna Cedulación.

La Dirección General del Registro Civil, Identificación y Cedulación de la República de Ecuador (DGRCIC) identificó y enfrento los siguientes retos relacionados con el proceso de cedulación en Ecuador:

- Ausencia de capacitación del personal.
- Un marco legal arcaico.
- Uso de tecnología obsoleta.
- Ausencia de mecanismos de auditoría avanzada, lo que aumentaba los actos de corrupción y malos manejos administrativos.

Por lo que a partir del 2007, se inició con el proceso de magna cedulación el cual, incluyó el uso de tecnologías como la construcción de edificios inteligentes y uso de unidades móviles.

El ciudadano o usuario, se registra por primera vez con el uso de una palabra secreta para abrir la red, proceso para el cual se implementó un sistema que toma la foto digital del usuario y su huella.

3. También en Ecuador, se cuenta con el programa de Dato Seguro.

   Portal que tiene como finalidad el compilar toda la información registral pública de diversas Instituciones del Ecuador, en donde cada ciudadano puede acceder de forma fácil y segura a su información.[24]

   Dicho portal además de tener la finalidad de que los ciudadanos consulten su información registral, también tiene el objetivo de que se pueda coordinar el intercambio de información de los registros públicos, así como también el que las entidades privadas que posean información que por naturaleza sea publica, son incorporadas en el sistema.

   Con lo anterior, se garantiza el acceso y consulta de los archivos públicos, garantizando la publicidad de la información y actos contenidos en los registros públicos, pero también se cuida la protección de la privacidad de la información de los ciudadanos, ya que para acceder al sistema, se solicita la confirmación del usuario y contraseña.

4. Portugal, se creó el Modelo de Interconexión del Registro Civil.

   En Portugal, se tenía la problemática se que en los municipios pequeños, las oficinas del Registro Civil también acumulaban otras funciones registrales, como es el caso del registro de inmuebles, de personas jurídicas o sociedades mercantiles y de vehículos.

   Por otra parte, es importante destacar que en Portugal, desde 1996 el registro civil de encuentra computarizado, de manera que el Registro Civil y los órganos de gobierno se encuentran interconectados para facilitar el trabajo registral.

   Un ejemplo del funcionamiento de este sistema, son los nacimientos, para los cuales los padres declaran el nacimiento, con lo cual se le asigna al niño un número de identificación y se interconectan los datos a través de internet, sistema que se encuentra disponible incluso en los hospitales privados. Además, en cuanto al registro civil, es importante destacar que se pueden realizar matrimonios y efectuar divorcios a través del sistema.

NECESIDAD DE UNA REFORMA LEGISLATIVA

Como hemos analizado, la publicidad de la información contenida en las bases de datos y documentos contenidos en los Registros Públicos, atiene a una necesidad de transparentar y dar publicidad a los actos en ellos registrados, sin embargo, conforme el acceso a tales registros se va aperturando y facilitando, el riesgo de extracción de información de los mismos con fines ilícitos también se incrementa y con ello se pone en riesgo la seguridad de la ciudadanía.

Es necesario generar reformas legales que ayuden a la implementación de nuevos sistemas que faciliten el resguardo y privacidad de los datos personales e información contenida en los Registros Públicos, estructuras que incluso, faciliten la interconexión entre plataformas de las dependencias de gobierno e instituciones privadas que manejan o generan estos Registros. Cuidando y respetando en todo momento el garantizar la publicidad de la información que caracteriza o forma parte de la esencia registral de los actos contenidos en los Registros Públicos.

Las reformas antes señaladas no solamente obedecen a la necesidad de aumentar los niveles de protección de los datos personales, sino que es importante analizar el hecho de que la mayoría de las normas que regulan la operación y funcionamiento de los Registros Públicos, fueron creados y entraron en vigor mucho tiempo antes de que las Tecnologías de Información y Comunicaciones tuvieran el auge y funcionalidades actuales, además de que también en su mayoría fueron creados antes de que entraran en vigor las normas de protección de datos personales, por lo que es muy lógico el hecho de que tales instituciones o registros públicos tengan oportunidades de mejora en cuanto a las posibilidades del uso de nuevas tecnologías tanto para la protección, manejo e incluso acceso a la información y datos en ellos contenidos, restructuras que a su vez tendrán que traer cambios legislativos que fundamenten su funcionamiento.

Como mencioné, al pensar en una reforma legislativa en esta materia, es importante que se considere el hecho de que las medidas de seguridad o sistemas de protección de datos personales que se establezcan para el acceso, operación o funcionamiento de los Registros Públicos no

tienen porque (i) limitar los derechos de acceso a la información y documentación pública gubernamental (transparencia), (ii) cancelar o ir en contra de las finalidades de publicidad frente a terceros de los Registros Públicos; o (iii) generar mayores cargas laborales o burocráticas a cargo de las instituciones públicas, privadas o de la ciudadanía.

Por lo anterior y después de analizar las mejores prácticas antes expuestas, una de las mejores formas de efectuar una reforma legislativa que permita el garantizar la publicidad de los datos personales contenidos en las bases de datos y documentos que se encuentran en los Registros Públicos, es el establecimiento de medios de control y consulta mediante los cuales se pueda identificar a la persona que realiza la consulta de la información, por medio de un usuario y contraseña o mediante cualquier otro medio de identificación y autenticación, como es el caso del portal de dato seguro en Ecuador, ello además de que se puede trabajar a la par la posibilidad de eficientar el acceso a la información mediante la consolidación de los archivos registrales de diversas dependencias en una sola plataforma o sistema, tomando como ejemplo las plataformas de Ecuador y de Portugal.

Es decir, establecer un sistema por medio del cual no se limite el acceso a los registros y fuetes públicas de información de las dependencias y registros públicas, pero por medio del cual si se deje un registro de las personas que consultaron extrajeron información o datos personales, con lo cual, en caso de incidencias o violaciones a la seguridad e integridad del titular de los datos personales, que sean ocasionadas por una violación a las disposiciones de protección de tales datos personales, el titular de los mismos pueda tomar acciones o conocer quienes fueron los que solicitaron acceso a sus datos personales y en su caso, los motivos por los cuales lo realizaron.

Además de lo anterior, es importante también el proponer como buena practica el caso de Perú, ya que al momento de establecer un sistema de identificación o autenticación ante los Notarios Públicos u otras autoridades, se pueden reducir de manera significativa los actos de usurpación de identidad que conllevan al ejercicio de actos delictivos en contra de los verdaderos titulares de los datos personales, lo cual, se podría complementar con el sistema de interconexión de documentos y datos personales de los registros públicos, antes mencionado.

CONCLUSIONES

Una vez analizado lo anterior, es importante destacar que la protección y privacidad de los datos personales de los ciudadanos es de vital importancia para la protección de los derechos de los ciudadanos, sea que tales datos estén bajo el tratamiento de las autoridades o de los entes privados.

Ahora bien, en relación al tratamiento de los datos personales que se encuentran bajo el tratamiento y responsabilidad de las autoridades, como ya vimos, los mismos están sujetos a confidencialidad, por lo que las autoridades deben garantizar su privacidad y protección. Restricción que a su vez cuenta con la salvedad de que en el caso de que dichos datos personales se encuentren en registros públicos o fuentes de acceso público, los mismos no estarán sujetos a dicha obligación de confidencialidad. Como es el caso de datos personales contenidos en los Registros Civiles, en los cuales, la consulta, trámite y obtención de las actas de nacimiento, matrimonio o defunción de encuentra a disposición de la ciudadanía.

Tales datos personales contenidos en las fuentes y registros públicos, se han visto impactados por el uso de las tecnologías de la información y comunicaciones por parte de los gobiernos o autoridades competentes, con lo cual, se han venido implementado plataformas, sistemas y estructuras que facilitan la consulta y acceso a la información y documentos en ellos contenidos.

Lo anterior, también ha sido empleado o puede llegar a ser empleado con efectos negativos, como es el caso de la extracción de información y construcción de perfiles con información obtenida de los registros públicos e incluso, pueden facilitar no solo la construcción de los perfiles sino también el que los delincuentes puedan adquirir documentación y archivos oficiales de dichas personas, con lo cual, fácilmente pueden suplantar la identidad de cualquier persona, o realizar actos en contra de su propia seguridad.

Algunos países como es el caso de Perú, Ecuador y Portugal ya han implementado diversos programas y sistemas que permiten disminuir los riesgos de que los datos e información personal

contenida en los registros públicos sea utilizada para el uso de delitos tales como el robo o usurpación de identidad, por ello, es conveniente analizar tanto sus antecedentes y problemáticas, así como las formas en las que resolvieron o disminuyeron estos riesgos para así poder analizar cual es la mejor práctica u opción que pudiera ser aplicable a cada uno de nuestros países, o incluso, si todas se pueden fusionar o adecuar a nuevas ideas y tendencias. Pero siempre velando por la privacidad de la información contenida en las bases de datos y archivos de los registros públicos, pero sin limitar el principio de publicidad que caracteriza a los registros públicos.

BIBLIOGRAFÍA

- Directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales, Convenio sobre la Organización para la Cooperación y Desarrollo Económicos, 23 de septiembre de 1980, http://inicio.ifai.org.mx/DocumentosdeInteres/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad.pdf.

- Convenio Nº 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Autormatizado de Datos de Carácter Personal, Consejo de Europa, 28 de enero de 1981, http://inicio.ifai.org.mx/DocumentosdeInteres/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf.

- Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico, APEC, 2005, https://www.sellosdeconfianza.org.mx/legal/Marco%20de%20privacidad%20APEC.pdf.

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, 24 de octubre de 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML.

- Ley Federal para la Protección de Datos Personales en Posesión de los Particulares, Cámara de Diputados del H. Congreso de la Unión, México, 05 de julio del 2010, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Cámara de Diputados del H. Congreso de la Unión, México, 08 de junio del 2012, http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf.

- Reglamento de la Ley Federal para la Protección de Datos Personales en Posesión de los Particulares, Cámara de Diputados del H. Congreso de la Unión, México, 21 de diciembre del 2011, http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf.

- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Cámara de Diputados del H. Congreso de la Unión, México, 11 de junio del 2003, http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf.

- Ley Federal de Archivos, Cámara de Diputados del H. Congreso de la Unión, México, 23 de enero del 2012, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFA.pdf.

- "En Michoacán, mínima protección de datos personales y sensibles", Quadratin Agencia Michoacana de Información y Análisis, http://www.quadratin.com.mx/politica/En-Michoacan-minima-proteccion-a-datos-personales-y-sensibles/.

- Diccionario de la Lengua Española, Vigésima Segunda Edición, Real Academia de la Lengua Española, http://www.rae.es/rae.html.

- Los Datos Personales en México, perspectivas y retos de su manejo en posesión de los particulares, Tenorio C., Guillermo, Editorial Purrúa, México 2012.

- Derecho Informático, Tellez V. Julio, Editorial McGrawHill, Cuarta Edición, México 2009.

- Consulta tu CURP, 2013, http://consultas.curp.gob.mx/CurpSP/.

- Registro Nacional de Profesionistas, Secretaría de Educación Pública, http://www.cedulaprofesional.sep.gob.mx/cedula/indexAvanzada.action.

- Obtén tu Número de Seguridad Social (NSS), INFONAVIT, http://portal.infonavit.org.mx/wps/wcm/connect/Infonavit/Trabajadores/Obten+tu+Numero+de+Seguridad+Social+(NSS)/

- Cuánto ahorro tengo, INFONAVIT, http://portal.infonavit.org.mx/wps/wcm/connect/infonavit/trabajadores/cuanto+ahorro+tengo/cuanto_ahorro_tengo.

- México, tercer lugar en robo de identidad, G. Ulloa Karina, Revista Sexenio, 30 de septiembre del 2013, http://www.sexenio.com.mx/articulo.php?id=39222.

- Registros Públicos, Una guía de privacidad para hispanohablantes, Privacy International, 2012, Londres Inglaterra, https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes/registros-publicos.

- Manual de practicas exitosas para el registro civil, Secretaría de Asuntos Políticos, Organización de Estados Americanos, Vol. 1, 2010, http://www.oas.org/es/sap/docs/puica/Manual_Buenas_Practicas_RegCivil.pdf.

- Manual de practicas exitosas para el registro civil, Secretaría de Asuntos Políticos, Organización de Estados Americanos, Vol. 2, 2011, https://www.oas.org/es/sap/docs/puica/Buenas_practicas_texto_completo_definitivo%20(2).pdf.

- Servicio de Verificación Biométrica del RENIEC, Cucho Espinoza, Mario, Lima, Perú, septiembre del 2010, http://www.cdi.org.pe/SemanaCalidad2010/presentaciones/J-SVB-RENIEC.pdf.

- Dirección Nacional de Registro de Datos Públicos, https://www.datoseguro.gob.ec/web/guest.

---

[1] Artículo 1º inciso b) de las Directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales; Artículo 2, inciso a) del Convenio Nº 108 del Consejo de Europa y el artículo 9 del Marco de Privacidad de APEC.

[2] Artículo 2, inciso a) de la Directiva 95/46/CE.

[3] Fracción II del artículo 3 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y fracción V del artículo 3 de la Ley Federal para la Protección de Datos Personales en Posesión de los Particulares.

[4] Artículo 1º de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

[5] Artículo 1º de la Ley Federal para la Protección de Datos Personales en Posesión de los Particulares.

[6] Privacidad, Real Academia de la Lengua Española, http://lema.rae.es/drae/?val=RAE.

[7] Artículo 7 de la Ley de Protección de Datos Personales en Posesión de los Particulares.

[8] Artículo 21 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

[9] Los Datos Personales en México, perspectivas y retos de su manejo en posesión de los particulares, Tenorio C., Guillermo, Editorial Purrúa, México 2012, p.p. 9.

[10] Artículo 7 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

[11] Los Datos Personales en México, perspectivas y retos de su manejo en posesión de los particulares, Tenorio C., Guillermo, Editorial Purrúa, México 2012, p.p. 11.

[12] Artículo 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

[13] Artículo 11 del Marco de Privacidad de APEC.

[14] Artículo 10 fracción II de la Ley de Protección de Datos Personales en Posesión de los Particulares.

[15] Derecho Informático, Tellez V. Julio, Editorial McGrawHill, Cuarta Edición, México 209, p.p. 36.

[16] "En Michoacán, mínima protección de datos personales y sensibles", Quadratin Agencia Michoacana de Información y Análisis, http://www.quadratin.com.mx/politica/En-Michoacan-minima-proteccion-a-datos-personales-y-sensibles/.

[17] Consulta tu CURP, 2013, http://consultas.curp.gob.mx/CurpSP/.

[18]Registro Nacional de Profesionistas, Secretaría de Educación Pública, http://www.cedulaprofesional.sep.gob.mx/cedula/indexAvanzada.action.

[19] Obten tu Número de Seguridad Social (NSS), INFONAVIT, http://portal.infonavit.org.mx/wps/wcm/connect/Infonavit/Trabajadores/Obten+tu+Numero+de+Seguridad+Social+(NSS)/

[20] Cuánto ahorro tengo, INFONAVIT, http://portal.infonavit.org.mx/wps/wcm/connect/infonavit/trabajadores/cuanto+ahorro+tengo/cuanto_ahorro_tengo.

[21] México, tercer lugar en robo de identidad, G. Ulloa Karina, Revista Sexenio, 30 de septiembre del 2013, http://www.sexenio.com.mx/articulo.php?id=39222.

[22] Manual de practicas exitosas para el registro civil, Secretaría de Asuntos Políticos, Organización de Estados Americanos, Vol. 1, 2010, http://www.oas.org/es/sap/docs/puica/Manual_Buenas_Practicas_RegCivil.pdf y Manual de practicas exitosas para el registro civil, Secretaría de Asuntos Políticos, Organización de Estados Americanos, Vol. 2, 2011, https://www.oas.org/es/sap/docs/puica/Buenas_practicas_texto_completo_definitivo%20(2).pdf.

[23] Servicio de Verificación Biométrica del RENIEC, Cucho Espinoza, Mario, Lima, Perú, septiembre del 2010, http://www.cdi.org.pe/SemanaCalidad2010/presentaciones/J-SVB-RENIEC.pdf.

[24] Dirección Nacional de Registro de Datos Públicos, https://www.datoseguro.gob.ec/web/guest.