REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.
ISSN 2530-4496 – AÑO 1, N° 1, 2016, PÁGS. 97-107

Protección de datos personales y TIC. Colisión permanente de derechos: utilización de periscope en la administración pública en México.

Protection of personal data and ICT. Permanent collision on rights: use of periscope in public administration in Mexico.

OLIVIA ANDREA MENDOZA ENRÍQUEZ

ABSTRACT

La incorporación de las tecnologías de la información y comunicación –en adelante TIC- a la administración pública en todos sus niveles, ha sido una característica de países como México. Es indudable los beneficios que estos servicios podrían traer a los ciudadanos, sin embargo, habrá elementos a considerar previo la utilización de dichas tecnologías en el sector público, particularmente tratándose de datos personales de los ciudadanos, que podrían ser transmitidos por un servidor público en tiempo real, sin la autorización del titular de dicho dato, o en el peor de los casos, cuando se trate transmisiones que incluyan la aparición de niños, niñas y adolescentes. Dicho lo anterior, será objetivo de este trabajo analizar los elementos a considerar para la utilización de TIC en el sector público, particularmente en el caso de *Periscope.*

I. INTRODUCCIÓN

De acuerdo con la Organización de Naciones Unidas, la revolución digital en las tecnologías de información y comunicación –en adelante TIC-, ha creado una plataforma para el libre flujo de la información, ideas y conocimiento en todo el planeta.[161] Esta revolución ha permitido nuevas formas de comunicación en tiempo real, como el caso de la tecnología en la cual sustentamos el análisis jurídico de las siguientes líneas.

Periscope ha representado una oportunidad idónea para que la gente pueda transmitir en tiempo real grabaciones que estime de interés para un público en lo particular. La aplicación forma parte de la red social *Twitter* y surgió con una idea de su creador Beykpour en un viaje a Turquía en 2013, año en el que se llevaron a cabo protestas en la plaza *Takshim* y al buscar información en línea de lo que sucedía para decidir si salía del hotel o no, encontró que no había plataformas que le permitieran a los usuarios del ciberespacio seguir en vivo las transmisiones desde el lugar.[162]

Periscope ha tenido un gran auge a partir de enero de 2016 que fue incorporado a la interfaz de *Twitter* y como en el caso de la mayoría de nuevas tecnologías, si bien su utilización tiene beneficios en la comunicación tales como la eliminación de las barreras de tiempo y espacio, su uso también ha planteado nuevos retos a la esfera jurídica, particularmente los relacionados a la privacidad y protección de datos personales, la determinación de competencia y jurisdicción en la materia, el consentimiento del titular de la imagen para ser transmitida, los límites de la libertad de expresión, el interés público, el principio de legalidad, el carácter vinculatorio de las resoluciones de las autoridades locales en materia de protección de datos personales, los flujos transfronterizos de dichos datos, etc.

En razón de lo anterior, el flujo de información hace necesaria la generación y aplicación de principios regulatorios, tanto a los medios de transmisión, como a los medios que contienen datos personales. En este sentido, debemos partir de la importancia de la información, ya que los datos personales tienen un valor significativo, el cual no está sólo relacionado al aspecto económico, sino al social, científico, político y cultural.[163]

En el contexto internacional se han emitido normas, iniciativas regulatorias, conferencias y directrices que han puesto al descubierto la relevancia de la protección de datos personales, tratando de dar una aproximación al tema; sin embargo, en el caso de las TIC, en la mayoría de ocasiones no ha sido su-

---

[161] TÉLLEZ, JULIO, Derecho Informático, México, McGraw-Hill, 2009, p. 1.

[162] Es importante anotar las casusas que dieron origen a Periscope, ya que atienden de manera similar al objetivo para el cual se utiliza en México.

[163] Véase REMOLINA, NELSON, Tratamiento de datos personales, aproximación internacional y comentarios a la Ley 1581 de 2012, Colombia, Legis, 2013, p. 3.

ficiente, ya que al ser un servicio relativamente nuevo, resulta complejo determinar por ejemplo, la jurisdicción aplicable en materia de datos personales respecto a la utilización de *periscope.*

Lo anterior se complica cuando *pericsope* es utilizado para fines de supervisión y documentación en la administración pública, ya que existen varios factores que considerar: si la persona que es grabada o que graba se encuentra en ejercicio de sus funciones, si en la grabación se transmite la imagen de un particular, si éste dio su consentimiento, si en el material aparecen niños, niñas o adolescentes, si el dispositivo con el que se graba es de uso oficial o personal, si existe una orden o sustento para llevar a cabo la transmisión, si la plataforma que se utiliza es propia y su manejo corresponde a alguna entidad del Estado, o en su caso, si corresponde a una plataforma particular que tiene su constitución fuera del país.

Dicho lo anterior, es momento de desarrollar el análisis de la problemática relacionada a la utilización de *periscope* en el sector público, los derechos en pugna, el marco jurídico aplicable, los elementos a considerar en los esquemas de protección de datos personales, resaltando que al tratarse de derechos humanos en conflicto, no pude dictarse una regla general, sino que en cada caso particular, deberá hacerse un ejercicio de ponderación de los mismos.

II. CONSIDERACIONES PREVIAS

Este trabajo busca centrarse en el derecho a la protección de datos personales, no obviando que existen otros derechos en conflicto derivado de la utilización de *periscope en* la administración pública en México.

La protección de datos personales surgió como una necesidad para garantizar los derechos humanos y facilitar el comercio dentro de sociedades democráticas. En este sentido, resulta importante primero decir que existen dos modelos principales de protección de datos en el mundo: el europeo y el americano.

Se debe precisar que los modelos de regulación son distintos a los sistemas de protección de datos personales, ya que los primeros hacen referencia a la forma de reglamentar, entre otras cuestiones, las obligaciones de los responsables del tratamiento así como los derechos de los titulares y los segundos, van más allá porque adicionalmente establecen mecanismos eficientes para que esos derechos y deberes se cumplan. En algunos casos se fusionan, pero esto es definido por cada país. En el caso de México tenemos un modelo híbrido, que retoma características tanto de Europa como de Estados Unidos de Norteamérica.

En este sentido, no todos los países asumen las mismas medidas de protección de datos personales, lo cual complica establecer la jurisdicción, particularmente hablando de situaciones de Internet.

Un elemento importante para entender la dinámica jurisdiccional digital, es establecer las diferencias entre los sistemas involucrados; es decir, las familias jurídicas a las que pertenecen los sujetos del servicio denominado *periscope*.

Desde el punto de vista político y económico, el debate se plantea entre los enfoques liberales, que proponen que las condiciones de mercado son las mejores garantías de la pluralidad y diversidad en la información, y aquellos que cuestionan esta hipótesis en beneficio de distintos grados y calidades de intervención de Estado y la sociedad civil; sin embargo, no es objetivo de este trabajo inclinarse hacia un determinado modelo de protección de datos personales.

De manera general, el sistema europeo se nutre de un conjunto de elementos jurídicos conformados

por normas generales y sectoriales con la figura de una autoridad de control encargada de hacer cumplir la regulación de la norma.

En esta tesitura, el Parlamento Europeo ha expresado que un sistema completo de protección de datos personales no requiere únicamente establecer los derechos de las personas cuyos datos se tratan y las obligaciones de quienes tratan dichos datos, sino también sanciones apropiadas para los infractores y un organismo supervisor independiente. De igual forma, el sistema europeo concibe la protección de datos como un derecho humano fundamental.[164]

Por otro lado, el modelo americano no considera la protección de datos personales como un derecho fundamental, sino como un derecho del consumidor. Está integrado por algunas disposiciones sectoriales y no estima necesaria la existencia de las autoridades de control especializadas en tratamiento de datos personales. Se inclina por la autorregulación y la promulgación de normas sectoriales, en lugar de disposiciones generales.

En Europa como se ha dicho, la protección de datos personales es considerada como un derecho fundamental, y por otro lado, en un ejemplo muy particular, la Constitución de los Estados Unidos de Norteamérica, no contiene una referencia explícita de la privacidad. En este país, la legislación de la privacidad, y en el caso de las leyes tradicionales, se enfocan en la protección de sus ciudadanos contra violaciones de las autoridades públicas y en Europa incluye al sector privado. Finalmente, decir que existe una divergencia fundamental entre las aproximaciones legales a la privacidad como un aspecto de libertad y la privacidad como un aspecto de dignidad.[165]

En el tema de jurisdicción, el modelo estadounidense perteneciente a la familia jurídica del *common law* tiene disposiciones relativas a la jurisdicción en los estatutos procesales y también son establecidas ampliamente por cada uno de los tribunales judiciales con base en la jurisprudencia y los precedentes existentes sobre la materia, bajo la doctrina *stare decis*, en la cual los jueces y magistrados están obligados a tomar en cuenta los precedentes establecidos en las decisiones judiciales anteriores.[166]

En el caso del modelo europeo, los países tienen un derecho codificado que cuenta con un Código Civil. Todas las resoluciones y sentencias sobre determinados casos son resueltas por los juzgados y tribunales judiciales conforme a la interpretación de las disposiciones contenidas en los códigos aplicables a cada materia y conforme a los hechos. [167]

Una vez que hemos hablado de los sistemas de protección de datos personales, debemos hablar de algunas consideraciones que nos permitirán entender el problema planteado.

La primera refiere a la jurisdicción aplicable en ámbitos digitales, ya que nos encontramos ante un servicio ofrecido por una empresa constituida en California (quien regirá sus prácticas conforme a la legislación de ese estado), con servidores establecidos en países terceros y con clientes o usuarios en todo el mundo. La complejidad se manifiesta cuando buscamos hacer vinculatorias las resoluciones emitidas por las autoridades locales, ya que al menos en el caso de México, eso no ha sido posible, ya que empresas como *Google Inc,* han desconocido la competencia del órgano garante en materia de protección de datos personales en el país, argumentando que la constitución legal del buscador se en-

---

[164] Reglamento CE 45/2011 del Parlamento Europeo.

[165] Véase RENDA, ANDREA, Cloud privacy law in the United States and the European Union, Regulating the cloud. Policy for computing infrastructure, Estados Unidos de Norteamérica, Instituto de Tecnología de Massachusetts, 2015, p. 135.

[166] Véase: VELASCO SAN MARTÍN, CRISTOS, La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet, México, Tirant, 2012, p. 217.

[167] Ibidem p. 241.

cuentra en Estados Unidos de Norteamérica.

Otra complejidad es que los datos (en el caso particular los videos), no se encuentran almacenados en servidores del país, lo cual se agrava al tratarse de datos personales de ciudadanos o de servidores públicos en el ejercicio de sus funciones.

Por otro lado, cada vez que se sube una fotografía o video de una persona a Internet, se está cediendo una seria de derechos sobre esta imagen al titular del sitio web y en ocasiones al resto de usuarios.[168]

La última complejidad de este análisis refiere en determinar hasta qué punto nos encontramos ante una violación del derecho humano de protección de datos personales en ámbitos digitales, ya que la mayor parte de vulneraciones son atribuidas a las empresas que prestan el servicio y no así a Estados en términos doctrinarios.

III. PROBLEMÁTICA

La nueva Delegada de Miguel Hidalgo perteneciente a la Ciudad de México, instruyó a la figura del *City Manager* llevar a cabo operativos que pudieran atender los principales reclamos de la ciudadanía en esa demarcación.

Con la finalidad de evidenciar el trabajo realizado, se optó por la utilización de *Periscope*, con el objetivo de transmitir en vivo los operativos, así como evidenciar a los propios servidores públicos cuando su actuación fuera contraria a la ley.

Las transmisiones se volvieron virales, particularmente cuando se hicieron operativos en residencias de figuras políticas pertenecientes al partido que hoy día gobierna el país. En ellas se puso al descubierto que algunas normas de tránsito no eran aplicables a los escoltas de dichas figuras. Ejemplo de ello es la disposición del Reglamento de Tránsito de la Ciudad de México que indica que solo vehículos oficiales podrían portar torretas, o aquella que indica la prohibición de estacionarse sobre banquetas que obstaculicen o impidan la libre circulación de peatones.

En este video el City Manager de la Delegación Miguel Hidalgo, se enfrentó a los escoltas quien de manera intimidatoria comentaron que tenían las autorizaciones necesarias para infringir las disposiciones de tránsito.

Cabe mencionar que el City Manager transmitía en vivo –a través de *Periscope*- este operativo y el enfrentamiento con los escoltas. En un momento de la grabación se apreció el interior de la residencia.

Después de estos hechos, el órgano garante del acceso a la información y protección de datos personales de la Ciudad de México, hablaba en los medios de una posible violación al derecho de protección de datos personales (imagen) de las personas transmitidas, mencionando que el servidor público no recabó el consentimiento de los titulares de los datos para ser transmitidos.

Derivado de lo anterior, se están discutiendo los lineamientos que delimiten la utilización de TIC en la administración pública de la ciudad de México.

IV. DERECHOS EN PUGNA

Los derechos en colisión son por una parte el derecho al honor, ya que derivado de las transmisiones podría afectarse este derecho, al señalarse como presuntos responsables de una falta o violación a la

[168] *TOURIÑO, ALEJANDRO, El derecho al olvido y a la intimidad en Internet, Madrid, 2014, p. 85.*

ley a determinados sujetos (servidores públicos o particulares), sin que ésta haya sido determinada por autoridad competente.

El derecho a la propia imagen que es un derecho relativamente nuevo en México. Esta vulneración atiende al detrimento que podría sufrir en su imagen una persona involucrada en las transmisiones, ya que son presentadas como infractoras y bajo un régimen de privilegios derivado de su condición o cargo en el país.

Por otra parte y a juicio de la autora, el derecho más importante en este caso concreto que es el derecho a la libertad de expresión, ya que las personas (en este caso servidores públicos) no podrían poner de manifiesto las situaciones que consideren afecten el interés público o colectivo.

En el mismo sentido, el derecho a la verdad que tenemos como personas de saber lo relativo a la función y ejercicio público y este derecho íntimamente relacionado al de acceso a la información reconocido en la Constitución Política de los Estados Unidos Mexicanos.

Finalmente el derecho a la protección de los datos personales que podría ser vulnerado derivado de transmisiones de este tipo.

Dicho lo anterior, cuando se trata de derechos en pugna como ya los mencionados, se deberá acudir a los ejercicios de ponderación, en los que se consideren por ejemplo, los principios del derecho de protección de datos personales, particularmente los relativos a la proporcionalidad y finalidad de la transmisión, para así acreditar que no se han excedido las funciones públicas en razón del objetivo que se persigue.

V. FUNDAMENTO JURÍDICO

El marco jurídico principal para el análisis de estas líneas son:

Declaración Universal de Derechos Humanos

Convención de los Derechos de los Niños

Constitución Política de los Estados Unidos Mexicanos

Ley Federal de Acceso a la Información Pública Gubernamental de 2002.

Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Lineamientos para la actuación en el uso, sociabilidad y operación de las Tecnologías de Información y Conocimiento (TIC), Plataformas y Redes Digitales en el Ámbito Gubernamental de la Ciudad de México, para la Protección de los Datos Personales, la Privacidad y Seguridad de las personas.

VI. PONDERACIÓN DE DERECHOS

Como hemos visto en el apartado anterior, son varios los derechos en pugna para resolver la interrogante respecto a si los servidores públicos están facultados para utilizar servicios como *Periscope* para la transmisión en vivo de operativos.

No es sencillo determinar la prohibición de la utilización de tecnología que permita la transmisión en vivo de algunos operativos en el cumplimiento de la función pública ya que si bien esta determinación protegería la imagen, honor y datos personales de los ciudadanos involucrados, también afectaría di-

rectamente al derecho de libertad de expresión[169] –elemento primordial de las sociedades democráticas, de acuerdo a la sentencia de 7 de diciembre de 1976 emitida por el Tribunal Europeo de Derechos Humanos contra Reino Unido- [170]; asimismo, existe un derecho de acceso a la información que encuentra su antecedente en el reconocimiento del derecho a la verdad[171] previsto en la Declaración Universal de Derechos Humanos de 1948.

Derivado de lo anterior, de deberá matizar que la tecnología empleada, debería ser una plataforma propia del Estado mexicano, que encuentre sus servidores en territorio nacional y que acate las reglas en materia de protección de datos personales del país. Si bien *periscope* no cumple con estos requisitos que otorgan certeza a la luz de derechos como el de protección de datos personales, si lo haría una plataforma institucional que prevea los principios y obligaciones en la materia.

Retomando el derecho a la verdad ligado con el de acceso a la información,[172] éste último ha sido reconocido en la Constitución desde 1977, en donde la Suprema Corte de Justicia de la Nación en el año 2000 ya se pronunciaba por la interpretación del mismo y en donde a partir del año 2002 se dota de la primera legislación en materia de acceso a la información en el país.[173]

Hoy día encontramos disposiciones en la Ley General de Transparencia y Acceso a la Información Pública del año 2015, respecto a la obligación de los sujetos de ese ordenamiento, de documentar todo lo relativo al ejercicio de la función pública, previendo también aquellos documentos que no se encuentren en medios tradicionales como el papel. En este sentido, prohibir la utilización de tecnologías que permitan documentar y evidenciar el día a día de los servidores públicos, resultaría incluso contradictorio a lo que indica esta ley sobre todo a los postulados del derecho de acceso a la información y a la rendición de cuentas en el país.

No omito mencionar que el derecho de acceso a la información encuentra su límite en el derecho a la protección de datos personales o en las reservas establecidas por la propia ley; sin embargo, en el caso de estos operativos no nos encontramos en supuestos de excepción, por lo que no contraviene las disposiciones hasta hoy promulgadas.[174] De igual forma, se deberán considerar los principios del derecho

---

[169] El Tribunal Europeo de Derechos Humanos ha establecido que incluso en estado de excepción, inestabilidad o guerra, el derecho a la libertad de expresión deberá prevalecer y el Estado tendrá la obligación de garantizarlo.

[170] Es interesante observar que cuando el derecho de libertad de expresión colisiona con otros, -no como regla general- pero en la mayoría de casos gana éste a la luz de derechos como el honor o la propia imagen. Ejemplo de ello lo encontramos en la resolución de 227 de febrero de 2001 emitida por el Tribunal Europeo de Derechos Humanos y por la que se condena a Austria. La determinación radicó en que a pesar de existir expresiones xenófobas en el dicho de un personaje público, debería prevalecer el derecho de libertad de expresión. Es interesante porque esto ejemplifica la sobrevaloración del derecho de libertad de expresión a la luz del derecho a la no discriminación.

[171] En este sentido, debemos recordar los Juicios de Núremberg, así como los lamentables hechos que dieron origen a los mismos, como un antecedente del reconocimiento del derecho a la verdad.

[172] Desde la región interamericana, la CIDH emitió un fallo paradigmático en materia de acceso a la información en el caso Claude Reyes vs Chile (el propio Tribunal Europeo de Derechos Humanos no lo había hecho), por el que el ciudadano demandó a ese Estado ya que solicitó información relativa a la autorización para construir un complejo en medio de una zona boscosa protegida y en donde el Estado Chileno negó el acceso a esa información argumentando que su Constitución no reconocía el derecho de acceso a la información. En términos generales la Corte obligó al Estado chileno a reconocer e incluir en su cuerpo normativo este derecho. También resulta importante decir que a diferencia del viejo continente, este órgano jurisdiccional no prevé el margen de apreciación de los Estados, lo cual atendiendo a la situación política e histórica de Latinoamérica no queda nada mal.

[173] Esta misma legislación es la que contiene disposiciones relativas a la protección de datos personales en el sector público y cabe mencionar que hoy día se discute la Iniciativa de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que dejaría sin efectos, en lo que respecta al derecho de protección de datos personales, al instrumento en comento.

[174] Se debe decir que no nos encontramos ante reservas de información, siempre y cuando se precise que los servidores públicos que pudieran aparecer en los videos, en supuestos casos de corrupción, se encuentran bajo la figura de "presuntos" infractores, ya que la autoridad competente deberá ser quien determine su responsabilidad.

de protección de datos personales, particularmente el relativo a la finalidad y proporcionalidad, así como los deberes en la materia, en especial el relativo a las medidas de seguridad en relación a la información.

En este sentido, la resolución del Tribunal Europeo de Derechos Humanos de 8 de julio de 1986 en el caso *vs* Austria, reconoció por primera vez dos libertades distintas: aquellas que consisten en expresar hechos que se pueden probar (definición de hechos) y aquellas opiniones o juicios de valor.

En este sentido, es importante decir que la documentación del día a día del ejercicio de la función pública no tiene prohibición expresa ni se contrapone con alguna otra legislación; sin embargo, si en el supuesto del que se trate, se evidenciara algún niño, niña o adolescente, y atendiendo al principio del interés superior del menor, se deberá salvaguardar la identidad del mismo y se omitirá cualquier dato que lo hiciera identificable. Aun pareciendo obvio, se debe decir que toda videograbación o transmisión en vivo, se deberá hacer desde un dispositivo oficial y no personal, a fin de evitar riesgos en torno a la privacidad, protección de datos personales e incluso la seguridad física de las personas involucradas.

Otro elemento a destacar es que en el caso planteado, existe un interés público o colectivo de conocer lo que pasa en dichos operativos, por lo que si se trata de un servidor público el que aparece en la transmisión, no será exigible el consentimiento de éste –como titular de su imagen- para aparecer en el video, ya que se trata de un representante del Estado que está en servicio y sobre todo que es susceptible del escrutinio público. En este sentido, no se puede suponer la misma interpretación tratándose de particulares, ya que en este caso, será necesario el consentimiento del titular de la imagen o al menos considerar que se cumplan con los principios del derecho de protección de datos personales.

En el ámbito europeo, el artículo 10 del Convenio Europeo de Derechos, prevé la libertad de expresión consagrada a través de la libertad de opinión y de la libertad para acceder a la información.

Como se dijo en líneas previas no existe una regla general para determinar qué derecho deberá prevalecer sobre otro, ya que en algunos casos, los datos de los ciudadanos si serán públicos.

Otra acotación importante es determinar si los particulares que aparecen en las transmisiones son personas públicas, cercanas a alguien público o totalmente del ámbito privado, ya que estas tres características constituyen categorías de análisis para determinar donde cede un derecho sobre el otro.[175]

Finalmente decir que en el caso de la utilización de *Periscope* en la administración pública, estamos ante transferencias internacionales de datos personales de ciudadanos mexicanos, por lo que deberíamos detenernos un poco a analizar lo que ha pasado en el ámbito europeo, con la Sentencia paradigmática de 2015, denominada Puerto Seguro.

En este sentido, los Lineamientos que propone el órgano garante de la protección de datos personales y acceso a la información de la Ciudad de México, hablan de información transferida, por lo que se deberá invocar las reglas internacionales de la transferencia de datos personales.

Retomando el tema de la Sentencia *Safe Harbor*, fue en octubre de 2015 cuando Europa opta por cesar la trasferencia de datos a Estados Unidos de Norteamérica, hasta que este país garantice las mismas condiciones de protección de la información de los ciudadanos europeos. Dicho lo anterior, y en una reivindicación de la interpretación del derecho a la protección de datos personales, la tendencia en el

---

[175] En este sentido el Tribunal Europeo de Derechos ha diferenciado entres las personas públicas, aquellas que las rodean y las que son personas meramente del ámbito privado. Un ejemplo de ello es que Pipa Middleton, hermana de la princesa Kate Middleton, ha perdido su lucha contra la prensa, al considerarse que la relación familiar con una figura de interés público en Inglaterra –como lo es la princesa-, la expone a vulneraciones en razón de su privacidad. En este ejemplo habrá que matizar si Pipa se encuentra en ámbitos públicos o privados, pero lo interesante es que en una ponderación de derechos se encuentra por encima aquel interés colectivo de saber, sobre el derecho a la privacidad de una persona, en razón de ser hermana de una figura pública.

viejo continente es reconocer un derecho amplio de protección de datos personales, por lo que en estos Lineamientos, no se puede retroceder, pensando en establecer aquello que se discutía en Europa hace más de una década.

VII. CONCLUSIONES

La utilización de nuevas tecnologías tanto en el sector público como privado tienen innumerables beneficios como la reducción de costos, la eficiencia en la administración y sobre todo la transparencia en el ejercicio de la función pública; sin embargo, su utilización se deberá hacer previo un riguroso análisis de los derechos en pugna, para así definir reglas claras que respeten los principios reconocidos en materia de protección de datos personales y de acceso a la información.

La implementación de nuevas tecnologías que permitan transmisiones en vivo a través de plataformas institucionales, resulta vital, a fin de otorgar certeza a los ciudadanos respecto al destino final de su información, así como de la jurisdicción aplicable que podría invocarse si existiera un problema legal. Resulta de vital importancia que las TIC implementadas en el sector público operen con sus propias plataformas, o en su caso con prestadores de servicios que reconozcan la jurisdicción mexicana o estén constituidos en el país. En el caso de *"periscope"* tecnología en la que se motivan estos lineamientos, su sede se encuentra en San Francisco, por lo que en los términos y condiciones de uso se indica que los problemas legales que del mismo se deriven, se tendrán que resolver en la jurisdicción estadounidense. Cabe mencionar que este argumento no ha sido sólido, ya que diversos países de Europa, como París, han determinado a través de la Suprema Corte que *Facebook* (empresa constituida también en Estados Unidos de Norteamérica), podría ser juzgado por jurisdicciones locales.

Es importante decir que los servicios locales permitirían el ejercicio de derechos ARCO (acceso, rectificación, cancelación y oposición) de los titulares de datos personales, ya que en ejemplos como la resolución del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) contra Google, Inc., se demostró que difícilmente las resoluciones del órgano garante nacional, serían vinculatorias para las grandes empresas de tecnología trasnacionales.[176]

Otro apunte necesario es que no en todos los casos se trata de derechos humanos en Internet. En la doctrina mexicana de derechos humanos, una característica de los mismos es que son exigibles a los Estados; sin embargo, en ámbitos digitales la exigibilidad de estos derechos no siempre es a los Estados mismos, sino a las grandes empresas trasnacionales que operan servicios informáticos y tecnológicos como *facebook, twitter, instagram*, etc. Derivado de lo anterior, nos encontramos ante las reglas de la *lex mercatoria,* más allá de las reglas de derechos humanos.

No obstante lo anterior, particularmente en el caso de Internet, ha servido como instrumento o herramienta de ejercicio de derechos humanos, ya que a través de éste podemos hacer valer nuestro derecho de libertad de expresión, pensamiento, asociación, etc.

El gran reto de la utilización de nuevas tecnologías en el sector público radica en lograr un equilibrio entre su utilización y la efectiva protección de derechos humanos como el de la privacidad, libertad de expresión y protección de datos personales.

Finalmente deberá ser el órgano garante a nivel nacional del derecho de protección de datos personales en México, quien se pronuncie y emita lineamientos de utilización de servicios de transmisión en vivo de imágenes, utilizados en la administración pública, a fin de que los servidores públicos conozcan la forma de conducirse cuando se haga empleo de este tipo de tecnologías. Este documento deberá incluir los principios del derecho de protección de datos personales a la luz de la transmisión de imágenes en tiempo real, así como los deberes en la materia.

---

[176] *La resolución puede ser consultada en: http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf*

FUENTES DE INFORMACIÓN

Bibliográficas:

RENDA, ANDREA, *Cloud privacy law in the United States and the European Union,* Regulating the cloud. Policy for computing infrastructure, Estados Unidos de Norteamérica, Instituto de Tecnología de Massachusetts, 2015.

REMOLINA, NELSON, *Tratamiento de datos personales, aproximación internacional y comentarios a la Ley 1581 de 2012*, Colombia, Legis, 2013.

TÉLLEZ, JULIO, *Derecho Informático*, México, McGraw-Hill, 2009.

TOURIÑO, ALEJANDRO, *El derecho al olvido y a la intimidad en Internet*, Madrid, 2014.

VELASCO SAN MARTÍN, CRISTOS, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet,* México, Tirant, 2012.

Legislativas:

Reglamento CE 45/2011 del Parlamento Europeo.

Páginas de Internet:

http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf

SOBRE LA AUTORA

OLIVIA ANDREA MENDOZA ENRÍQUEZ es Doctora en Derecho, Maestra en Derecho con especialidad en Derecho Económico y Licenciada en Derecho por la Benemérita Universidad Autónoma de Puebla.

Se desempeña como docente e investigadora de jornada completa en el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC) en Ciudad de México, México.

Su correo electrónico es: olivia.mendoza@infotec.mx

Este trabajo fue recibido el 24 de junio y aprobado el 14 de julio de 2016.