INTERNET, PRIVACIDAD Y DATOS PERSONALES. EL DEBATE A PARTIR DE LA REFORMA CONSTITUCIONAL EN MATERIA DE TELECOMUNICACIONES Y RADIODIFUSIÓN

MARÍA ELENA MENESES ROCHA

Libertades en Internet

Internet se ha convertido en un entorno propicio para que los ciudadanos expresen sus ideas políticas y pidan rendición de cuentas a los gobernantes. Se trata de un instrumento crucial en el siglo XXI que potencia las libertades democráticas (La Rue, 2014). La red, según el exrelator para la Libertad de Expresión de las Naciones Unidas, Frank La Rue, facilita el acceso a la información e incrementa la observancia ciudadana para que las instituciones rindan cuentas y faciliten la activa participación ciudadana en la construcción democrática. Así, en países en donde prevalecen libertadas acotadas, las potencialidades democráticas disminuyen.

A nivel mundial, las libertades en Internet han disminuido en el último lustro. Según el reporte de la organización Freedom House (2015), las amenazas se han generalizado en los últimos años con la promulgación de tratados comerciales y leyes que comprometen la potencialidad que tiene la Red como instrumento para el ensanchamiento de estas libertades. La organización que evalúa a sesenta y cinco países encontró que en cuarenta y dos los gobiernos piden a las empresas restringir o borrar contenidos políticos y religiosos; en cuarenta, se envió a prisión a personas que compartieron información sobre estos temas y en catorce se decretaron leyes que incrementan la vigilancia sobre los ciudadanos.

Entre el Estado, las empresas y los usuarios hallamos tensiones recurrentes que amenazan esta tríada de derechos interrelacionados: libertad de expresión, derecho a la información y derecho a la privacidad. Este último es el que resulta más vulnerado con la creciente digitalización de la sociedad y a partir del cual se enfrentan los mayores desafíos de orden jurídico, político y social.

En el presente texto se expone el inédito debate alrededor de estas tensiones a partir de la reforma constitucional en materia de Telecomunicaciones y Radiodifusión de 2013 con el fin de documentar e identificar los puntos y argumentos fundamentales de la discusión, no solo para ofrecer un recuento histórico, sino para promover el análisis y un debate más amplio tendiente a buscar las mejores prácticas que tengan como eje los derechos civiles y políticos con una mirada multidisciplinar que busque el fortalecimiento de la democracia.

En el mundo, se debate alrededor de la creciente tentación de los Estados para que los concesionarios de telecomunicaciones y proveedores de aplicaciones y contenidos funjan como intermediarios ya sea para criminalizar a los internautas que violen derechos de autor, ya para retener datos personales sin controles rigurosos, con el fin de perseguir delitos en ocasiones sin ordenamientos judiciales, con el riesgo latente de desproteger al ciudadano frente al Estado.

La creciente importancia de estos intermediarios ha hecho necesario establecer responsabilidades, pues son mediadores que posibilitan las prácticas sociales, culturales y políticas de la sociedad actual. La conectividad es posible gracias a estos intermediarios que tienen control sobre la infraestructura, el acceso, los contenidos y las prácticas de los usuarios; son por tanto de diversa índole y por eso se hace necesaria una tipología de estos sujetos regulables, como la que proponen Ruiz Gallardo y Lara Gálvez (2012):

- Proveedores de conexión, que son los que brindan acceso a Internet, conexión e infraestructura.
- Proveedores de alojamiento, que son los que ponen a disposición de otros la posibilidad de mantener contenidos en la Red.
- Proveedores de contenido, que son quienes brindan a los usuarios diversos contenidos o servicios sean o no provistos por ellos mismos.

El Pacto por los Derechos Civiles y Políticos de la Organización de las Naciones Unidas en sus artículos 17, 18 y 19, respectivamente —así como los países firmantes, como México con el artículo 16 constitucional—,

señalan que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud del mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

Si bien el marco legal es imprescindible, no es suficiente para la protección de derechos en tensión constante dada la complejidad y la diversidad de los diferentes campos de acción de los actores involucrados, así como su marco contextual, metas, fines y propósitos que dificultan la articulación de consensos a la hora de elaborar reglas y criterios de colaboración (Nissenbaum, 2011).

El acceso a Internet como derecho fundamental

Diversos gobiernos, conscientes de que Internet es más que una infraestructura, han incorporado a sus respectivos marcos constitucionales el acceso a la Red como derecho. Se trata de un debate mundial que parte del reconocimiento de que las formas de interrelación humana han cambiado y se han trasladado a un tercer entorno o ambiente digital (Echeverría, 1999; Benkler, 2006). Tal entorno requiere, como señala Javier Bustamante (2010), garantizar derechos humanos de cuarta generación, que son los que amplían la noción de ciudadanía a la nueva realidad tecnológica de la cual se desprenden nuevos problemas, realidades y desafíos.[1]

El tercer entorno tiene su materialidad en los proveedores de servicios antes señalados, denominados en la legislación mexicana como "Concesionarios de telecomunicaciones y proveedores de servicios de aplicaciones y contenidos", los cuales son sujetos de regulación en todo el mundo, dada su centralidad y poder como agentes mediadores entre el usuario y el tercer entorno, y que son causa de un debate a escala local y global pues hay quienes consideran que deben ser eximidos de responsabilidad, salvo en casos de excepción.

1 Para el filósofo español Javier Bustamante, los derechos humanos de primera generación son el derecho a la dignidad y autonomía frente al Estado; los de segunda generación son los de naturaleza económica y social que exigen la intervención pública del Estado como el derecho a la salud y la educación, y los de tercera generación los relacionados con los derechos colectivos y de algunas minorías. Los de cuarta generación serían aquellos que se desprenden de la nueva realidad tecnocientífica.

En México, por iniciativa del Ejecutivo y con el consenso de todas las fuerzas políticas del país, el Congreso modificó en 2013 el artículo 6º de la Constitución para garantizar a los ciudadanos el acceso a los servicios de telecomunicaciones e Internet de banda ancha como un derecho fundamental, además de considerarlos servicios públicos de interés general. Esta reforma abrió el debate sobre los derechos humanos de cuarta generación en el país relacionados con el tercer entorno.

Materializar el derecho de acceso a un servicio público de interés general ha sido un camino lleno de obstáculos, retos y lecciones para el presente y futuro de la construcción ciudadana en México, así como para el establecimiento de una política digital alejada de determinismos. El papel de los intermediarios ha sido objeto de análisis y disenso, pues de las decisiones que les involucran y de las competencias que se les atribuyen depende en buena medida el marco de libertades antes aludido.

Acceso, retención de datos personales, geolocalización y neutralidad de la Red se han tornado en fenómenos emergentes de renovada complejidad, al involucrar una multiplicidad de actores y campos de acción que provocan un desafío para la elaboración de leyes y regulaciones. En este proceso jurídico, político y tecnosocial, se observa una superposición de metas y objetivos multidisciplinarios y contextuales que vuelven difícil la conciliación de derechos y ante lo cual se hace necesario que antes de legislar se busquen consensos de una manera multisectorial, incluyente y negociada.[2]

Aun cuando la aprobación de las leyes de la trascendente reforma constitucional de 2013 debió tener lugar a más tardar en diciembre de ese mismo año, fue hasta 2014 cuando el Ejecutivo envió su propuesta de dictamen de ley secundaria. Ésta, de acuerdo con diversos sectores sociales, era en diversos aspectos contraria a la reforma en cuestión que en sí misma representaba un hito y detonador de desarrollo digital para el país.

Sin ser el único aspecto relevante y preocupante en aquella propuesta de ley secundaria enviada por la Presidencia de la República, los artículos sobre la colaboración con la justicia por parte de los proveedores de

2 En el presente texto se analizan únicamente la geolocalización, la retención de datos personales y contenido de comunicaciones privadas.

Internet, de aplicaciones y de contenidos fueron los más polémicos. Organizaciones civiles y ciudadanos instrumentaron una campaña en redes sociales a través de los *hashtags* #EPNvsInternet, #Nomaspoderalpoder y #Contraelsilenciomx que dio lugar a que los senadores y el propio gobierno escucharan los argumentos de lo que era sin lugar a dudas una contrarreforma.

Esta movilización potenció una protesta dentro y fuera de la Red, lo que obligó a la Cámara de Senadores a revisar la iniciativa del Ejecutivo, para lo cual convocó a organismos de la sociedad civil, académicos y ciudadanos para exponer su punto de vista y debatir en el recinto legislativo. El tema más controversial fue la redacción y las posibles implicaciones del artículo 197 de aquella propuesta que contemplaba "bloquear, inhibir o anular de manera temporal las señales de telecomunicaciones en eventos y lugares críticos para la seguridad nacional a solicitud de las autoridades competentes" (DOF, 2014b), artículo relacionado con tres asuntos que se discuten en el presente texto: la geolocalización en tiempo real, la cual se refiere a búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada; la retención de datos personales que concierne a la conservación de metadatos por parte de los proveedores; así como el contenido de las comunicaciones privadas (DOF, 2015).

Dicha iniciativa intentaba legitimar el espionaje gubernamental por intermediación de los proveedores sin ningún tipo de control. Luego de la protesta social y una vez que los senadores escucharon propuestas y argumentos en contra, en el mes de abril de ese año, se realizaron algunas modificaciones y adiciones.[3] Finalmente, en la Ley Federal de Telecomunicaciones y Radiodifusión, decretada en julio de 2014, el bloqueo de señales en sitios públicos quedó limitado a perímetros alrededor de los penales, sin embargo, otros temas quedaron igual y representan un debate inaplazable de los derechos humanos en el tercer entorno en México, como la geolocalización o localización geográfica de equipos de comunicación sin la mediación de ordenamientos judiciales, así como la retención de

3 Una de las propuestas presentadas que finalmente fue retomada por los senadores para ser incorporada en la ley fue la relacionada con la accesibilidad de los servicios de telecomunicaciones y radiodifusión para las personas con discapacidad.

datos personales por parte de los proveedores. Por mandato de la ley correspondió al Instituto Federal de Telecomunicaciones (IFT) emitir las disposiciones administrativas que habrán de regir la colaboración entre los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos con las instancias de procuración de justicia.

Luego de las protestas, la neutralidad de Internet —un derecho que puede ser considerado de cuarta generación, ya que supone un conjunto de principios que deben ser garantizados por los proveedores de servicios de telecomunicaciones y de contenidos y aplicaciones tales como la libre elección y no discriminación de tráfico y contenidos— quedó plasmada en los artículos 145 y 146 (Ley Federal de Telecomunicaciones y Radiodifusión, 2014).

El concepto de "neutralidad", acuñado por el investigador estadounidense Tim Wu (2003), considera que este derecho tiene repercusiones para el ejercicio de la libertad de expresión al evitar condicionamientos o limitaciones por parte de los proveedores con criterios comerciales o políticos (Red en Defensa de los Derechos Digitales, 2015). Aunque para el real cumplimiento de esta obligación se requiere no sólo de mecanismos y lineamientos específicos, que se espera sean emitidos en 2016, sino de la consciencia de los consumidores de sus propios derechos, su incorporación a la ley en la materia puede considerarse un importante avance en beneficio de los usuarios.

Privacidad y retención de datos personales

La vida contemporánea pasa por el tercer entorno, lo cual genera riesgos para la privacidad ya que todo lo que ocurre ahí deja una huella imborrable: los datos. Todo ciudadano tiene derecho a tener una esfera privada resistente a las injerencias arbitrarias del Estado o de terceros, lo cual requiere de dos políticas vinculadas con la protección de este derecho fundamental en toda sociedad democrática: el derecho a tener un discurso anónimo y a la protección de los datos personales.

Las empresas de la economía digital retienen datos para compartir con terceros y los Estados para fines que van desde la seguridad pública hasta la seguridad nacional. Este resguardo por parte de los proveedores

de servicios de Internet, de servicios de aplicaciones y contenidos, se ha convertido en tema de preocupación recurrente. Conscientes de la responsabilidad de los intermediarios y preocupados por la incomprensión del entorno Internet por parte de diversos gobiernos, los relatores especiales para la libertad de expresión de Naciones Unidas y de la Comisión Interamericana de los Derechos Humanos, el representante de la Organización para la Seguridad y Cooperación en Europa (OSCE) y la relatora especial para la Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos (CADHP) emitieron en 2015 una serie de consideraciones sobre la creciente vigilancia de los gobiernos que afectan el derecho a la libertad de expresión, el derecho a la información y la privacidad.

De acuerdo con los expertos el tema merece un equilibrio adecuado entre el orden público y las necesidades de seguridad y los derechos de libertad de expresión y privacidad. En el documento condenan la retención de datos personales de forma indiscriminada y establecen criterios que toda autoridad debe seguir para garantizar: transparencia, supervisión independiente y derecho a la encriptación de comunicaciones personales (OEA, 2015). La declaración de los relatores podría ser considerada como valiosa guía para los tomadores de decisiones al momento de legislar y elaborar reglamentos sobre el tercer entorno.

En México, el artículo 16 de la Constitución garantiza el derecho a la protección de datos personales, el cual establece los supuestos de excepción a los principios que rijan el tratamiento de datos, "por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros". Se entiende por datos personales "cualquier información concerniente a una persona física identificada o identificable" y datos personales sensibles a aquellos que afecten a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

En particular, se consideran datos sensibles aquellos que puedan revelar "aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual" (DOF, 2010: 2).[4] Así, los datos

4 De acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de

personales se encuentran protegidos tanto por la Constitución como por los Tratados Internacionales, de los cuales México es signatario, por lo que su conservación indiscriminada interfiere con el derecho a la privacidad y al cuidado de datos personales (Red en Defensa de los Derechos Digitales, 2014).

Tanto la Constitución como la Ley de Protección de Datos garantizan la privacidad de los ciudadanos. Sin embargo, en su artículo 189, la Ley Federal de Telecomunicaciones en su apartado "Colaboración con la Justicia" mandata a los concesionarios de telecomunicaciones y proveedores de servicios de aplicaciones y contenidos a la geolocalización de aparatos móviles en tiempo real y a "conservar un registro y control de comunicaciones" que se realicen desde cualquier tipo de línea; esto incluye todo tipo de comunicación: mensajes, mensajes cortos, multimedia y lo que denomina sin especificar "avanzados". Obligación que merece ser analizada por sus posibles consecuencias sobre los derechos aludidos.

La retención de datos permite rastrear e identificar el origen y destino de las comunicaciones; modalidad de pago de la línea; fecha, día y hora de cuando se llevó a cabo y de la primera activación del servicio. La entrega de los datos deberá hacerse en tiempo real a las autoridades que lo soliciten, para lo cual los concesionarios están obligados a retener doce meses los metadatos en medios que permitan su consulta inmediata. Una vez cumplido este lapso están obligados a guardar doce meses más dichas bases en sistemas de almacenamiento electrónico.

En julio de 2014, doscientas dieciocho organizaciones civiles pidieron al Instituto Federal de Acceso a la Información y Protección de Datos Personales (IFAI) interponer una acción de inconstitucionalidad ante la Suprema Corte de Justicia de la Nación y defender así los derechos de privacidad y protección de datos personales ante la nueva ley.

El Instituto Federal de Acceso a la Información Pública y Protección de Datos Personales analizó el caso y descartó por mayoría de votos interponer la acción de inconstitucionalidad, porque según el órgano los artículos 189 y 190 no atentan contra la Ley de Protección de Datos Personales. Una decisión controversial porque para muchos ciudadanos

---

los Particulares, que fue publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010, tras ser aprobada el 13 de abril de ese año.

las disposiciones de los artículos mencionados representan una injerencia arbitraria a la privacidad de los mexicanos.

La Constitución Política en el artículo 16, en concordancia con la Comisión Interamericana de Derechos Humanos (CIDH), considera que la retención de datos sólo es viable en casos excepcionales y mediante ordenamientos judiciales. En la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) en el artículo 189 se señala que:

> Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes.

En el artículo 190 se establece que están obligados a conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que se utilice, numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:

1. nombre, denominación o razón social y domicilio del suscriptor;
2. tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);
3. datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;
4. datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;
5. además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;
6. en su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

7. la ubicación digital del posicionamiento geográfico de las líneas telefónicas, y
8. la obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación (artículo 190, LFTR, 2014).

La retención de datos por parte de concesionarios y proveedores de servicios de Internet y de aplicaciones y contenidos repercute en una mayor vulnerabilidad cuando es indiscriminada y con escasos controles, sobre todo si no fija ningún criterio objetivo que garantice que las autoridades nacionales competentes son las únicas que tendrán acceso a los datos y si no se especifica qué delitos ameritan acceder a ellos. Cuando dichos proveedores fungen como intermediarios, son mucho mayores los riesgos que los beneficios que pueden obtenerse, siendo la retención sólo plausible en situaciones extraordinarias y bien delimitadas y autorizadas por un juez.

Si bien como hemos sostenido los datos personales y su protección son atribuciones del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el IFT fue el órgano encargado de la emisión de los criterios con los cuales se llevará a cabo la retención de datos en el país bajo los principios de legalidad, debido proceso, notificación al usuario y la mediación de una autoridad competente. Contradicciones y empalme de facultades y atribuciones que son una muestra de la complejidad de este tema emergente en México. Los lineamientos de colaboración de los proveedores en materia de seguridad y justicia fueron emitidos por el IFT a finales de 2015, luego de una consulta pública.[5]

Lineamientos de colaboración en materia de seguridad y justicia

El 2 de diciembre de 2015 finalmente fueron publicados en el *Diario Oficial de la Federación* los lineamientos expedidos por el IFT responsa-

5 La Ley General de Transparencia y Acceso a la Información Pública entró en vigor el 5 de mayo de 2015 con lo cual el IFAI pasó a ser el Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos Personales (INAI).

ble de expedir las reglas, los mecanismos y los procedimientos para una efectiva colaboración. De acuerdo con el IFT, del 12 al 27 de noviembre de 2015 se recibieron en la consulta pública diecinueve participaciones de personas morales y nueve de personas físicas, entre las que destacan las cámaras que agrupan a los sujetos regulados, quienes opinaron sobre el proceso de implementación de los mecanismos y medios para la gestión de requerimientos de información geolocalizada en tiempo real y de datos conservados establecidos en los artículos 189 y 190, respectivamente (DOF, 2015).[6]

El IFT tomó en cuenta algunos señalamientos de los sujetos regulados y de organismos de derechos humanos sobre la gravedad de conservar el Número de Identificación Personal de Servicio Contratado (NIPSC), decisión que representa un avance producto del diálogo, además de la consideración de las recomendaciones del Consejo Consultivo del IFT en ese sentido; no obstante los lineamientos prevén una serie de medidas que podrían desproteger a los ciudadanos frente al Estado al no acotar y precisar restricciones en materia de derecho a la privacidad.

Los lineamientos, que aplican a partir de 2016, apelan al marco jurídico en materia de protección de datos personales y enfatizan que cualquier mal uso de estos será objeto de las sanciones civiles y penales aplicables. De esta forma, el IFT solo estableció las bases de la colaboración que le mandata la ley, limitaciones que se pueden traducir en desprotección para los ciudadanos, quienes podrían acogerse a la figura de amparo como único recurso en caso de ver vulnerado su derecho a la privacidad.

Los lineamientos fueron precedidos de un estudio de impacto regulatorio limitado a realizar recomendaciones de gestión y de un breve análisis comparado de la geolocalización, retención de datos e intervención de las comunicaciones en el mundo. El estudio carece de una mirada amplia ya que sólo pondera y se alinea con el Plan Nacional de Desarrollo del gobierno del presidente Enrique Peña Nieto en relación con la prevención social de la violencia y la delincuencia (IFT, 2015b).

6 Se dará prioridad a las situaciones en donde se encuentre en peligro la vida de una persona y a las amenazas a la Seguridad Nacional.

Así, el estudio y los lineamientos parten de un diagnóstico sobre la criminalidad en el país, basado en datos cuantitativos y cualitativos provenientes de diversos organismos, con lo cual justifica la necesidad de regular a este grupo de actores dada la centralidad de la comunicación móvil en la consecución de delitos como el secuestro sin aludir al disenso y al debate internacional en relación con los derechos en disputa.

De acuerdo con el estudio el IFT señala que se hace necesaria: *a*) la geolocalización, *b*) la retención de datos por veinticuatro meses a partir del momento en que se origina la comunicación y *c*) la intervención de comunicaciones privadas, para este punto en específico contempla la autorización de un ordenamiento judicial (DOF, 2015).

En ningún momento se consideran las consecuencias y reparación de daños de una eventual intromisión en la privacidad, tanto como de una posible inhibición del uso de Internet en un país en el que falta mucho por hacer para conseguir el acceso a los servicios de telecomunicaciones e Internet de banda ancha —derecho consagrado en el artículo 6º—, así como la necesidad de impulsar la educación digital para que los ciudadanos se apropien de la tecnología para el desarrollo personal y social, ante lo cual un entorno hipervigilado por el Estado puede resultar contraproducente.

Los concesionarios y autorizados tendrán que tener áreas especializadas disponibles veinticuatro horas al día los 365 días al año para atender las solicitudes de las autoridades facultadas. Para la solicitud y entrega los lineamientos se contemplan Plataformas Electrónicas y el establecimiento de Grupos de trabajo para facilitar la colaboración. A los concesionarios y autorizados se les responsabiliza de asegurar la disponibilidad continua de la plataforma electrónica y de garantizar la seguridad de la misma (DOF, 2015).[7] Esta excesiva transferencia de responsabilidades no estuvo exenta de cuestionamientos por parte de los sujetos regulables, los más afectados y, por tanto, quienes mantuvieron una presencia importante en la consulta pública sobre los lineamientos. La Asociación Mexicana

7 Los "autorizados" son quienes tienen un título habilitante para establecer y operar una comercializadora de servicios de telecomunicaciones sin tener el carácter de concesionarios.

de Internet (Amipci) estimó que por concepto de la conservación de los datos por dos años tendrán que invertir quinientos millones de dólares con consecuencias inciertas sobre el costo de los servicios con cargo al usuario (Guerrero, 2014).

Según la comisionada del IFT Adriana Labardini, "en su voto particular, los lineamientos eximen a las Autoridades Facultadas de establecer protocolos de seguridad estrictos y certificados en una plataforma única, permitiendo así sistemas alternativos y opcionales para requerir la información por distintas vías con lo cual el instituto señaló la Comisionada, "claudica a su misión de tutelar derechos de los usuarios" (Labardini, 2015). Además, en los lineamientos, no se ofrece un listado de autoridades facultadas con lo cual los regulados habrán de decidir si el requerimiento "proviene de una autoridad debidamente facultada o no", lo cual no otorga certeza a los concesionarios, lo que según la comisionada que expresó su inconformidad con diversos apartados, es "inaceptable" entre otras cosas por la precaria situación de la procuración de justicia en México.

Entre otras obligaciones se estableció el número de emergencia 911 a nivel nacional existente en otros países como Estados Unidos, Canadá, Argentina, Uruguay, entre otros, así como el establecimiento de algunas obligaciones para las autoridades facultadas, las cuales deberán informar dos veces al año los requerimientos realizados y el registro de datos de comunicaciones cancelados y suprimidos de manera segura, una vez cumplido el fin para lo cual fueron solicitados (DOF, 2015), información que a su vez será publicada en el portal del instituto.[8]

En caso de que los datos hayan sido vulnerados sólo se establece la obligación de notificar a los usuarios para "contrarrestar" cualquier afectación sin contemplar el derecho de notificación referida a las personas afectadas por medidas de vigilancia encubierta, tal como lo recomendó el Consejo Consultivo del órgano regulador el 23 de febrero de 2015 (Consejo

8 En el capítulo X de los lineamientos se establece que el IFT debe integrar un comité especializado de estudios e investigaciones con el objeto de desarrollar soluciones tecnológicas para inhibir el uso de equipos de telecomunicaciones para la comisión de delitos.

Consultivo IFT, 2015). Mínimas obligaciones para las autoridades facultadas en contraste con un exceso de responsabilidades para los proveedores, así como el riesgo de vulnerabilidad del ciudadano frente al Estado caracterizan los lineamientos que si bien incorporaron un necesario número de emergencia 911 y la intervención de órdenes judiciales para el caso de la intervención de comunicaciones privadas, están aún lejos de garantizar plenamente el respeto a la privacidad de los ciudadanos.

Delegar a los particulares la compleja preservación de los datos resulta riesgoso para la privacidad, tanto como las limitaciones autoimpuestas por el IFT para fungir como un auténtico mediador y establecer límites a la vigilancia gubernamental con criterios más rigurosos, certificados y únicos con el fin de evitar vulnerar derechos fundamentales.

La retención de datos en la Unión Europea

El debate aquí expuesto tiene lugar en todo el mundo. Luego de los atentados en Madrid en 2004 y en Londres en 2005, la Unión Europea autorizó la retención de datos para facilitar las acciones contra el terrorismo. Después de años de discusiones y evaluaciones entre los Estados miembros de la Unión y ante la inconformidad de países como Alemania, Irlanda y Austria con esta normativa, en 2014 el Tribunal de Justicia de la Unión Europea decidió que la retención de datos "se inmiscuye de manera especialmente grave en los derechos fundamentales al derecho a la vida privada y a la protección de datos de carácter personal" (Tribunal de Justicia de la Unión Europea, 2014).

En 2010, luego de un intenso debate que terminó en una acción colectiva con 34 000 firmas, Alemania declaró la retención de datos como anticonstitucional. Diversas evidencias sustentan la decisión del Parlamente Europeo. De acuerdo con el informe de la unesco de 2012, "Internet Privacy and Freedom of Expression", hubo una fuga de datos del sistema postal de veinticinco millones de personas en Gran Bretaña e Irlanda del Norte. A mediados de 2011, la empresa coreana SK Communications admitió la pérdida de datos de 35 000 000 de personas, equivalente al 85 por ciento de los usuarios de Internet en ese país.

En México, en 2009, 98 400 000 líneas telefónicas fueron dadas de alta en un programa gubernamental obligatorio, el Registro Nacional

de Usuarios de Telefonía Móvil (Renaut), junto con las respectivas claves de registro único de población, el curp de los usuarios que es la clave de identidad de los ciudadanos mexicanos. El gobierno se había comprometido a que estarían resguardados por la Secretaría de Gobernación para el combate a la delincuencia. Las bases de datos acabaron a la venta en diversos sitios de Internet y al gobierno le llevó un año su destrucción (Monroy, 2012).

El Tribunal Europeo, luego de analizar casos como estos, prohibió la retención de datos relativos a comunicaciones y a información consultada y conservó la normativa de retención de tráfico, localización e identificación del usuario por un lapso mínimo de seis meses y máximo de dos. Sostuvo que la retención al ser indiscriminada a toda la población usuaria de algún servicio de telecomunicaciones, pone también en riesgo el control de dichos metadatos. ¿Qué seguridad tienen los usuarios de dispositivos y plataformas de que sus datos no serán robados, filtrados o utilizados para fines no autorizados? Se preguntaron con razón los parlamentarios europeos.

De esta forma, los parlamentarios acordaron que "la conservación de los datos para su posible transmisión a las autoridades nacionales competentes responde efectivamente a un objetivo de interés general (la lucha contra la delincuencia grave y la seguridad pública), sin embargo, estimaron que al adoptar la Directiva sobre la conservación de datos, el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad" (Tribunal de Justicia de la Unión Europea, 2014). No obstante, el Tribunal reconoció algunas limitantes de su decisión, por ejemplo, la imposibilidad de controlar la retención de datos en un solo país dado el carácter transnacional de la Red y de las empresas proveedoras, con lo cual el cómputo en la nube y el Internet de las cosas se tornan en temas que requieren una mirada amplia de los actores involucrados y estudiosos del fenómeno.[9]

La decisión del Tribunal Europeo se dio luego de las develaciones de Edward Snowden y de la inconformidad de países europeos con Estados

9 Concepto que se refiere a la interconexión de objetos a Internet por medio de datos.

Unidos por su proyecto de vigilancia de la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés) que involucra a empresas de la economía digital como las de telecomunicaciones y de redes sociales, entre las que se encontraba Facebook. Sin embargo, y como muestra de un debate inacabado, en 2015, algunos países tomaron decisiones controversiales al legislar a favor de la vigilancia del Estado.

El caso más relevante es el de Francia, que luego de los ataques al semanario *Charlie Hebdo* aprobó, por una abrumadora mayoría la Asamblea Nacional, una ley de inteligencia para reforzar medidas a favor de la retención de datos y la vigilancia de las comunicaciones de los ciudadanos. La decisión causó críticas de organismos de derechos humanos franceses que argumentaron, entre otras cosas, la falta de controles de la comisión encargada (La Quadrature du net, 2015). Otro es el caso de Gran Bretaña —aliado de Estados Unidos en Europa—, cuyos parlamentarios conservadores y laboristas apoyaron el Proyecto de Ley de Poderes de Investigación, la IP Bill, que permite la retención de datos por doce meses y la interferencia de comunicaciones siempre y cuando sea autorizada por el Ministerio del Interior (UK Parliament, 2015).

La ONU no ha estado ajena al debate, en 2015 hizo un llamado a considerar el cifrado de datos y el anonimato como un derecho fundamental y llamó a las naciones a establecer debates transparentes para garantizarlos y prever medidas de excepcionalidad en casos específicos lo cual es una cuestión impostergable en México.

Reflexiones finales

La LFTR en México, decretada en julio de 2014, está lejos de haber cumplido las expectativas de todos los actores involucrados. En cuanto al tercer entorno, el tema pendiente es conciliar la seguridad y el combate al crimen con la privacidad de los ciudadanos, lo cual amerita mirar más allá de los planes de desarrollo y periodos gubernamentales.

Queda en la agenda nacional incorporar a la red a setenta millones de ciudadanos, con lo cual toda disposición contraria a respetar y proteger el marco de derechos civiles y políticos pueden limitar su utilización. Internet no es sólo un entorno para cometer delitos, sino que se trata

de un instrumento para la democracia, potencialmente educativo y que favorece la productividad.

Si algo positivo dejó la prolongada discusión de la Ley en México fue el activo social incuantificable conformado por ciudadanos decididos a interpelar y demandar un Internet libre de posibles abusos por parte del Estado que pueden impedir la articulación de un bien común digital que ensanche las libertades civiles y políticas. La agenda en México sobre el complejo tercer entorno es muy amplia. Como señalan juristas y estudiosos de la red como habilitadora de desarrollo humano, la mejor forma de regular Internet es mediante una jurisprudencia más negociada y cooperativa que la observada hasta ahora, sin demeritar el inédito, difícil y perfectible proceso seguido por el IFT para cumplir con el mandato constitucional.

La grave situación de violencia por la que atraviesa el país resulta insuficiente como criterio único cuando puede ser incompatible con los derechos humanos, para lo cual hace falta una discusión más amplia que incorpore a más actores y estudios especializados de las consecuencias de esta vigilancia en diversos ámbitos de la vida social. Vigilar en nombre de la seguridad nacional exige una definición clara del concepto y también sus dimensiones y delimitaciones. Demanda no dejar a los ciudadanos vulnerables frente al poder de Estado.

FUENTES

Álvarez, C.

2013 *Derecho de las Telecomunicaciones*. Ciudad de México: Fundalex y Posgrado de Derecho, UNAM.

2104 "Algunos puntos inconstitucionales, incongruentes o que contravienen el interés público de las iniciativas de leyes secundarias de telecomunicaciones presentadas por el presidente Enrique Peña Nieto el 24 de marzo de 2014", *Hechos y derechos*, 2 de abril, en <http://biblio.juridicas.unam.mx/revista/HechosyDerechos/cont/20/art25.htm>, consultado el 1° de diciembre de 2015.

Benkler, Y.

2006 *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press.

Bustamante, J.

2010 "La cuarta generación de derechos humanos en las redes digitales", *Telos*, en <https://telos.fundaciontelefonica.com/url-direct/pdf-generator?tipoContenido=articuloTelos&idContenido=2010110411480001&idioma=es>, consultado el 30 noviembre 2015.

Consejo Consultivo del IFT

2015 "Recomendaciones del Consejo Consultivo del Instituto Federal de Telecomunicaciones respecto al anteproyecto de lineamientos en materia de colaboración de seguridad y justicia", 23 de febrero, en <http://consejoconsultivo.ift.org.mx/docs/others/Recomendacion_Lineamientos_de_Colaboraci%C3%B3n-Seguridad_y_Justicia.pdf>, consultado el 27 de febrero de 2016.

Diario Oficial de la Federación (DOF)

2015 "Acuerdo mediante el cual el pleno del Instituto Federal de Telecomunicaciones expide los 'Lineamientos de colaboración en materia de seguridad y justicia' y modifica el plan técnico fundamental de numeración", *Diario Oficial de la Federación*, 21 de junio de 1996, en <http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015>, consultado el 27 de febrero de 2016.

2014a "Decreto por el que se expiden la Ley Federal de Telecomunicaciones y Radiodifusión y la Ley del Sistema Público de Radiodifusión del Estado Mexicano y se reforman, adicionan y drogan diversas disposiciones en materia de telecomunicaciones y radiodifusión", en <www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014>.

2014b "Iniciativa de decreto por el que se expiden la Ley Federal de Telecomunicaciones y el Sistema Público de Radiodifusión de México y se reforman y adicionan y derogan diversas disposiciones en materia de Telecomunicaciones y Radiodifusión", en <http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014>, consultado el 5 de noviembre de 2015.

2014c "Ley Federal de Telecomunicaciones y Radiodifusión", *Diario Oficial de la Federación*, 14 de julio.

2011 "Capítulo I de los Derechos Humanos y sus Garantías", *Diario Oficial de la Federación*, 10 de junio.

2010 "Ley Federal de Protección de Datos Personales en Posesión de los Particulares", *Diario Oficial de la Federación*, 5 de julio.

Echeverría, J.

1999 *Los señores del aire: Telépolis y el Tercer Entorno*. Barcelona: Destino.

Estañol, A.

2014 "IFAI descarta ir contra #LeyTelecom", *CNN Expansión*, 13 de agosto, en <http://www.cnnexpansion.com/negocios/2014/08/13/ifai-descarta-ir-en-contra-de-leytelecom>, consultado el 14 de septiembre de 2015.

European Commission

2014 *Protection of Personal Data*, en <http://ec.europa.eu/justice/data-protection/>, consultado el 5 de noviembre de 2015.

Franceschi-Bicchierai, L.

2013 "The Delicate Balance between Internet Freedom and Big Data", *Mashable,* 25 de septiembre, <http://mashable.com/2013/09/25/big-data-internet-freedom/>, consultado el 5 de noviembre de 2015.

Freedom House

2015 *Freedom on the Net 2015*, en <https://freedomhouse.org/report/freedom-net/freedom-net-2015>, consultado el 5 de noviembre de 2015.

García, L.

2015 *Vigilancia estatal de las comunicaciones y protección de los derechos fundamentales en México*, en <https://www.eff.org/files/2015/12/17/mexico-sp-dec2015.pdf>, consultado el 1° de diciembre de 2015.

García, L. F. Y C. Brito

2014 "Enrique Peña Nieto contra el Internet", *Nexos*, 31 de marzo, en <http://www.redaccion.nexos.com.mx/?p=6176>, consultado el 5 de noviembre de 2015.

Global Pulse

2013 "Our Privacy and Data Protection Principles", *Global Pulse*, en <http://www.unglobalpulse.org/privacy-and-data-protection>, consultado el 5 de noviembre de 2015.

Guerrero, V.

2014 "Exigen frenar espionaje", *Amipci*, <https://www.amipci.org.mx/es/noticiasx/2219-exigen-frenar-espionaje>, consultado el 27 de noviembre de 2016.

Instituto Federal de Telecomunicaciones (ift)

2016 "Acuerdo mediante el cual el Comisionado presidente del Instituto Federal de Telecomunicaciones establece el Comité Especializado de Estudios e Investigaciones en Telecomunicaciones a que se refiere el Capítulo X de los lineamientos de colaboración en materia de Seguridad y Justicia y designa a los servidores públicos que formarán parte del mismo", en <http://www.ift.org.mx/sites/default/files/acuerdo_comite_especializado_20160114.pdf>, consultado el 27 de febrero de 2016.

2015a "Acuerdo mediante el cual el pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración", publicado el 21 de junio de 1996, en <http://www.ift.org.mx/sites/default/files/conocenos/pleno/sesiones/acuerdoliga/dofpiftext111115159.pdf>, consultado el 27 de febrero de 2016.

2015b "Anexo A", *Análisis de impacto regulatorio*, en <www.ift.org.mx/sites/default/files/industria/temasrelevantes/379/documentos/airseguridadyjusticiafinal11nov2015.pdf>, consultado el 27 de febrero de 2016.

2015c "Voto razonado sobre el asunto enlistado bajo el numeral III.1 de la orden del día de la XLIII sesión extraordinaria de 'Acuerdo mediante el cual el pleno del Instituto Federal de Telecomunicaciones que expide los lineamientos de colaboración en materia de seguridad y justicia y modifica el plan técnico fundamental de numeración' publicado en el dof 21 de junio de 1996, sesión extraordinaria", en <http://www.ift.org.mx/sites/default/files/voto_escrito_labardini_p_ift_ext_111115_159.pdf>, consultado el 27 de febrero de 2016.

2014a *Comunicado*, en <www.ift.org.mx/iftweb/wp-content/.../COMUNICADO-ITEL-280214.pdf>, consultado el 5 de noviembre de 2015.

2014b "Consulta pública sobre el 'Anteproyecto de Lineamientos de colaboración en materia de seguridad y justicia'", en <http://www.ift.org.mx/industria/consultas-publicas/consulta-publica-sobre-el-anteproyecto-de-lineamientos-de-colaboracion-en-materia-de-seguridad-y>, consultado el 27 de febrero de 2016.

2014c "Respuestas generales que proporciona el Instituto Federal de Telecomunicaciones a las manifestaciones, opiniones, comentarios y propuestas presentadas durante la consulta pública del: Acuerdo mediante el cual el pleno del Instituto Federal de Telecomunicaciones aprueba someter a consulta pública el 'Anteproyecto de lineamientos de colaboración en materia de seguridad y justicia'", en <http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/379/documentos/respuestasconsultapublicafinal.pdf>, consultado el 27 de febrero de 2016.

Instituto Nacional de Estadística y Geografía (inegi)

2013 *Módulo de uso y disponibilidad de tecnologías de información y comunicación en los hogares, MODUTIH*, en <www.inegi.org.mx/inegi/contenidos/espanol/.../2013/.../comunica46.pdf>, consultado el 5 de noviembre de 2015.

Internet World Statistics

2013 *Internet Usage Statistics: World Internet Users and Population Stats*, en <http://www.internetworldstats.com/stats.htm>, consultado el 5 de noviembre de 2015.

La Rue, F.

2014 *Principios sobre libertad de expresión en la era digital. Informe de la Relatoría Especial para la Libertad de Expresión 2013*, 16 de junio, en <http://www.oas.org/es/cidh/expresion/temas/internet.asp>, consultado el 5 de noviembre de 2015.

Labardini, A.

2015 "*V*oto Particular sobre el asunto enlistado bajo el numeral III.1 de la orden del día de la XLIII sesión extraordinaria", en <http://www.ift.org.mx/sites/default/files/voto_disidente_labardini_p_ift_ext_111115_159.pdf>, consultado el 27 de noviembre de 2015.

Quadrature Du Net

2015 "L'Assemblée nationale vote la surveillance de masse des citoyens français!", *La Quadrature du Net*, 5 de mayo, en <https://www.laquadrature.net/fr/

lassemblee-nationale-vote-la-surveillance-de-masse-des-citoyens-francais>, consultado el 26 de diciembre de 2016.

Mendel, T., A. Puddephatt, B. Wagner, D. Hawtin y N. Torres

2012 "Global Survey on Internet privacy and freedom of expression", *unesco Series on Internet Freedom*, en <http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/global-survey-on-internet-privacy-and-freedom-of-expression/>, consultado el 6 noviembre de 2015.

Meneses, M.

2014 *La vigilancia del Estado en tiempo de la red ubicua. Libertad de Expresión, Disidencia y Democracia*. México: Instituto Belisario Domínguez Senado de la República.

Meza, S.

2014 "cisen, con un ojo en las redes sociales", *El Universal*, 19 de agosto, en <http://archivo.eluniversal.com.mx/nacion-mexico/2014/cisen-con-un-ojo-en-las-redes-sociales--1031385.html>, consultado el 8 de septiembre de 2015.

Monroy, J.

2012 "Tomará un año destruir el Renaut", *El Economista*, 9 de mayo, en <http://eleconomista.com.mx/sociedad/2012/05/09/tomara-ano-destruir-renaut>, consultado el 8 de septiembre de 2015.

Nissenbaum, H.

2011 *Privacidad amenazada: tecnología, política y la integridad de la vida social*. México: Océano.

Notimex

2010 "Exigen a PGR indagar venta de Renaut", *El Universal*, 11 de junio, en <http://www.eluniversal.com.mx/notas/687086.html>, consultado el 5 de noviembre de 2015.

Organización de Estados Americanos (oea)

2015 *Declaración conjunta sobre la libertad de expresión y las respuestas a las situaciones de conflicto*, 4 de mayo, en <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=987&lID=2>, consultado el 12 de septiembre de 2015.

Organización de las Naciones Unidas (onu)

1966 *Pacto por los Derechos Civiles y Políticos*, en <http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx>, consultado el 12 de septiembre de 2015.

Red en Defensa de los Derechos Digitales

2015 *Neutralidad de la Red en México: del dicho al hecho*, en <https://s3.amazonaws.com/f.cl.ly/items/3K2T3v0b452g0a1C0d2E/R3D%20-%20Neutralidad%20de%20la%20red%20en%20Mexico%202015.pdf>, consultado el 5 de noviembre de 2015.

2014 "Consulta pública del anteproyecto de lineamientos de colaboración en materia de seguridad y justicia", en <http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/consultaspublicas/documentos/comentariosr3dconsultaift.pdf>, consultado el 27 de febrero de 2016.

Ruiz, C. Y J. Lara

2012 "Responsabilidad de proveedores de servicios de Internet (ISP) en relación con el ejercicio del derecho de libertad de expresión en Latinoamérica", en E. Bertoni, eds., *Hacia una Internet libre de censura. Propuestas para América Latina*. Buenos Aires: Universidad de Palermo.

Tribunal de Justicia de la Unión Europea

2014 "El Tribunal de Justicia declara inválida la 'Directiva sobre la conservación de datos'", 8 de abril [comunicado de prensa], en <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf>, consultado el 5 de noviembre de 2015.

UK Parliament

2016 *Joint Committee on the Draft Investigatory Powers Bill Draft Investigatory Powers Bill, Report of Session 2015-16*, 11 de febrero, en <http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/9302.htm>, consultado el 27 de octubre de 2016.

Unión Internacional de telecomunicaciones (UIT)

2014 "Measuring the Information Society", *MIS Report 2013*, en <http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2013.aspx>, consultado el 5 de noviembre de 2015.

United Nations Human Rights

2015 *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of opinion and expression, David Kaye*, en <http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/USA.pdf>, consultado el 5 de noviembre de 2015.

Wu, T.

2003 "Network Neutrality, Broadband Discrimination", *Journal of Telecommunications and High Technology Law* 2: 141, en <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863>, consultado el 27 de diciembre de 2016.