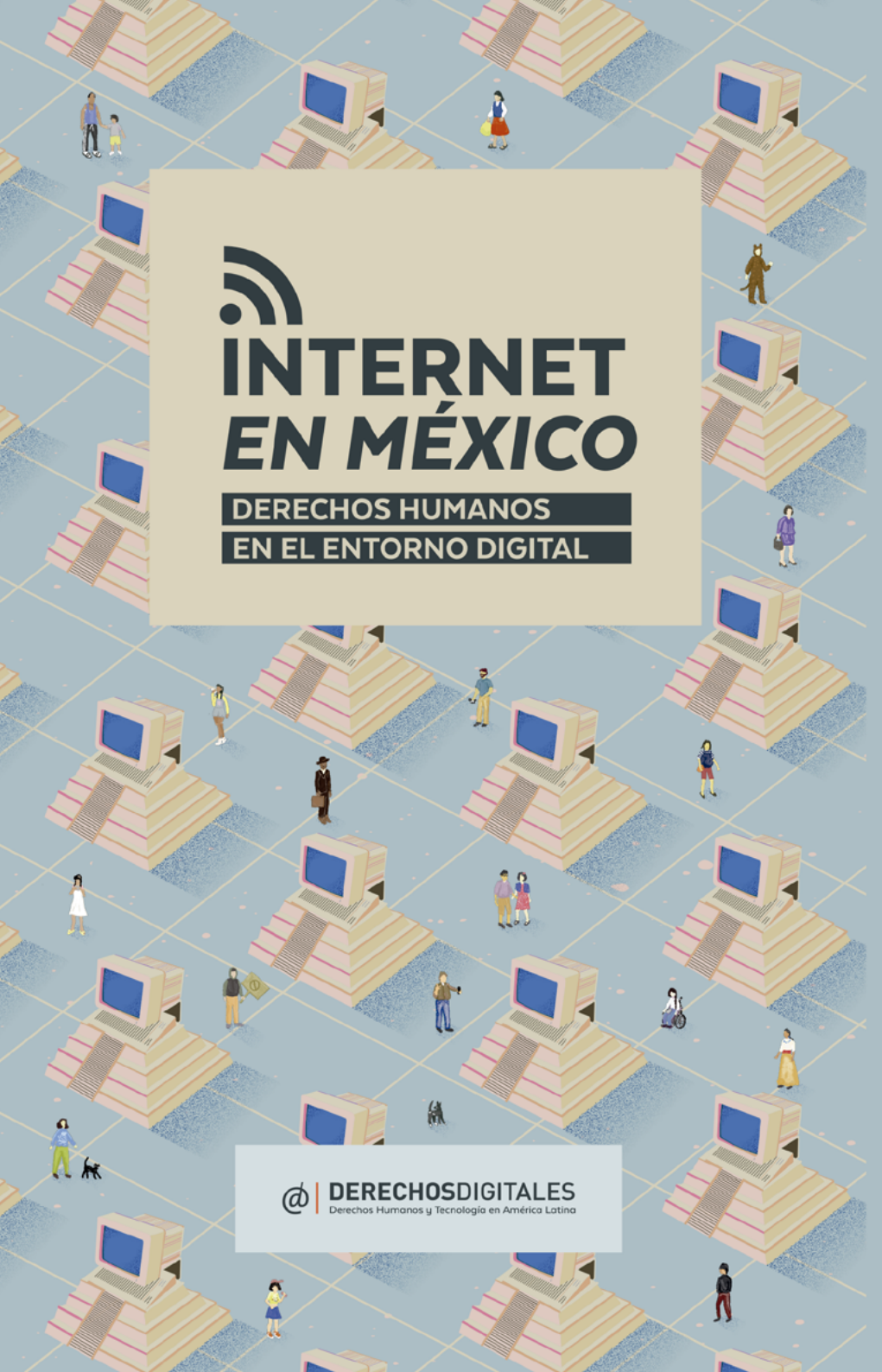


INTERNET *EN MÉXICO*

DERECHOS HUMANOS EN EL ENTORNO DIGITAL

@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina

INTERNET *EN MÉXICO*

DERECHOS HUMANOS EN EL ENTORNO DIGITAL

Internet en México: Derechos Humanos en el entorno digital
Editado por Derechos Digitales.
Impreso en México, 2016.

Edición general por Juan Carlos Lara.
Coordinación editorial de Gisela Pérez de Acha.
Correcciones de Paz Peña y Vladimir Garay.
Portada y Diagramación por Constanza Figueroa.

Esta publicación de Derechos Digitales ha sido posible gracias al apoyo de Global Partners Digital y Google Inc..

Oficina central:
Diagonal Paraguay 458, piso 2, Santiago de Chile.
Código postal: 855003
Fono: (+56 2) 2702 7108
derechosdigitales.org
info@derechosdigitales.org

INTERNET *EN MÉXICO*

DERECHOS HUMANOS EN EL ENTORNO DIGITAL

@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina

Índice

Introducción

Hace poco más de una década, hablar de derechos humanos en internet desde América Latina parecía un ejercicio un tanto forzado: se trataba de tecnologías con muy limitado acceso por la población, aparentemente útil para una cantidad restringida de tareas, con un potencial gigantesco pero cuyos desafíos regulatorios palidecían a la luz de los requerimientos de justicia social durante las últimas décadas del siglo pasado. Hoy, en cambio, una gran parte de nuestra vida social, laboral, cultural y económica se desarrolla a través de las tecnologías. Hoy, mucho del potencial de la red se ve materializado en las interacciones de millones de usuarios y usuarias y de la forma en que ejercemos derechos básicos mediados por lo digital.

Particularmente en nuestra región, durante los últimos años hemos visto que estas tecnologías maravillan a tomadores de decisiones. Como si por ciertas características ocultas, estos dispositivos permitieran de manera automática la mejora de las condiciones materiales de nuestra sociedad y su sola adopción nos acelerara el camino al desarrollo. Sin embargo, estos espacios también suponen un arma de doble filo. Es cierto, por un lado, que la masificación de medios digitales ha permitido el uso de plataformas nunca antes vistas en la historia para organizarnos y amplificar nuestros mensajes. Esto implica una oportunidad, quizás única, para el desarrollo de derechos como la libertad de expresión, información, asociación, reunión, entre otros. Pero al mismo tiempo, estas nuevas tecnologías suponen una ame-

naza latente. El espionaje y la censura son más fáciles y menos costosas que antaño y, además, las desigualdades y esquemas de discriminación se han traducido también al mundo online con sus propias particularidades y problemas inherentes.

Sin ir más lejos, el proyecto que dio vida hace ya más de diez años a Derechos Digitales comenzó en Chile tratando de influir en las nacientes políticas públicas digitales y en aquellas que vinculaban la tecnología con el ejercicio de derechos civiles, en un rincón de la región con una turbulenta historia reciente en materia de derechos humanos, con fuertes tensiones sociales y políticas, y con una progresiva narrativa de seguridad más amplificada que los discursos sobre libertades y garantías, todo lo cual parecía traspasado al entorno digital. Cuando decidimos expandir nuestro trabajo al resto de la región, nos encontramos no solamente con un lenguaje común e historias afines, sino también con fuertes tensiones sobre la lectura, el ejercicio y la defensa de los derechos fundamentales.

En pocos lugares esas tensiones son tan palpables como en México. La complejidad política, la seria crisis de derechos humanos y los constantes cuestionamientos institucionales por parte de la sociedad civil ameritan un análisis serio, que abone al debate democrático, pensando en las oportunidades que entrega internet para el ejercicio de los derechos humanos desde el contexto local.

Actualmente, los regímenes legales no dan cuenta de la rapidez con la que se mueven las nuevas tecnologías y sus consecuencias. Frente a este desfase, el fenómeno regulatorio en México

es muy particular, sobre todo desde el movimiento estudiantil #YoSoy132, que propuso una narrativa que confrontaba al poder desde la internet misma. Más que producto de una escasez de conocimiento de los legisladores, las leyes que se han promovido denotan una aproximación con temor a este medio: un espacio descentralizado que da cabida y permite amplificar los discursos más críticos. De la lectura de algunas propuestas pareciera que internet, en particular, requeriría una regulación urgente, como una forma de resolver un espacio opaco, donde no reinaría el estado de derecho sino el caos del insulto anónimo. Los debates en torno a la Ley Telecom y la Ley Fayad son tan solo dos ejemplos que ilustran lo anterior.

Por esa razón, hacer un libro en México no es fortuito ni es un mero capricho. ¿Cómo regular la tecnología para permitir que se fortalezcan nuestros derechos y se eviten los abusos? ¿Cómo idear políticas públicas que permitan la protección del disenso y la construcción de una democracia robusta? Ambas preguntas son el eje central de este libro y sus respuestas se buscan desde las leyes y la realidad política de México.

Con esto en mente, este libro busca una aproximación a los fenómenos regulatorios desde una perspectiva de políticas públicas para proponer estrategias, oportunidades y distintos lineamientos de regulación en cada materia. Para llegar a ello, hemos reunido a diversos personajes de la vida pública mexicana que, por su especial trayectoria, reflexionan sobre seis distintos temas: anonimato, violencia de género, vigilancia de las comunicaciones privadas, protesta social, neutralidad de la red y gobierno abierto.

Cada autor y autora expresa su visión desde México, con la mirada puesta en las reglas del futuro para fenómenos actuales que vinculan derechos fundamentales y tecnologías. Se trata de temas complejos, con múltiples aristas tanto globales como locales. Autoras y autores expresan su propia opinión y sus propios argumentos, que no coinciden necesariamente con la visión de Derechos Digitales pero que, sin duda, aportan al enriquecimiento de los debates sobre internet en México. Todas, discusiones que pese a parecer a veces abstractas o lejanas tienen impactos reales sobre la vida de las personas y el ejercicio de sus derechos. El solo hecho de plantear sus opiniones para esos debates y ponerlas a disposición del público, constituye un avance importante que agradecemos. Más reflexiones en el ambiente permiten un debate público más honesto, informado y robusto.

En el capítulo denominado "En defensa del anonimato", coescrito por Antonio Martínez Velázquez y José Flores Sosa, los autores dan cuenta de una de las discusiones más actuales en el ámbito de internet: ¿es el anonimato una herramienta para la libertad de expresión o un mecanismo que fomenta el abuso y las actividades criminales? En este capítulo se argumenta cómo la economía actual en línea se preocupa por la construcción de un "perfil del consumidor" de múltiples servicios a partir de la recopilación masiva de sus datos en la red, mismos que se monetizan y se venden como publicidad. Las preguntas son amplias y complejas. ¿Cómo proteger el derecho al anonimato desde aquí? ¿Qué papel juega el anonimato frente a la tradición impuesta por el Ejército Zapatista de Liberación Nacional y la criminalización de las "capuchas" por parte del gobierno?

¿Qué lineamientos deben seguirse para también respetar y garantizar derechos de otros terceros?

Estefanía Vela Barba y Erika Smith tratan un tema pocas veces abordado desde una perspectiva de políticas públicas: "La violencia de género y las tecnologías de la información". Las autoras reflexionan acerca de la violencia de género en línea, los derechos humanos que se afectan y, sobre todo, qué soluciones se requieren para atender a las víctimas sin promover la censura en internet. El capítulo hace notar cómo siguen operando los viejos estereotipos de género en las nuevas tecnologías, abordando fenómenos tristemente extendidos como la difusión no consentida de imágenes íntimas, las amenazas, la difamación, el acecho o el acoso, en muchos casos con un fuerte componente sexual y de violencia. La reflexión se complementa con casos paradigmáticos como el de Menstruadora, una activista feminista que se vio obligada a cerrar sus redes sociales, y la madre de Axan, que recibió amenazas de muerte luego de permitir a su hijo llevar el cabello largo a la escuela.

En el capítulo "La vigilancia y su impacto en el derecho a la privacidad en México", Luis Fernando García y Jesús Robles Maloof cuestionan una narrativa muy común en los gobiernos de nuestra época: cómo el discurso de seguridad justifica las intromisiones en el derecho a la privacidad de nuestras comunicaciones. Se dice que para poder combatir el crimen deben implementarse medidas de vigilancia como la interceptación de llamadas y mensajes, la geolocalización o la instalación de software malicioso en nuestros teléfonos y computadoras. Uno de los problemas principales es que estas medidas suponen un

alto poder invasivo, al mismo tiempo que, por su propia naturaleza, son invasiones secretas, que puede prestarse a serios abusos por las autoridades. En este sentido, ¿cuáles son las leyes más problemáticas en el derecho mexicano? ¿Qué lineamientos de política pública deben seguirse entonces para equilibrar los derechos en juego y disminuir la arbitrariedad? Los autores indagan en estas preguntas y esbozan algunas respuestas.

Alberto Lujambio Llamas y José David Aroesti Ventura tratan "La criminalización de la protesta social" en México, tanto en el mundo analógico como en el mundo digital. Históricamente, el aparato político mexicano ha reprimido el disenso y los movimientos sociales en sus diversas manifestaciones, como ocurrió en la matanza de Tlatelolco en 1968, con el Ejército Zapatista de Liberación Nacional, con #YoSoy132 y con los movimientos de solidaridad por la desaparición de los 43 normalistas de Ayotzinapa. Frente a este gran aparato represor, internet ha sido una herramienta de amplificación expresiva y organización simultánea a través de *trending topics*, *hashtags*, *likes* y memes de plataformas como Twitter y Facebook. Si la protesta es esencialmente pública, ¿podemos esperar que estos espacios digitales, controlados por privados, respeten una expresión pública? Para proponer lineamientos y ejes de política pública, los autores toman como base la "Declaración conjunta sobre libertad de expresión e internet" con el fin de establecer parámetros que permitan el disenso.

En el capítulo "Neutralidad de la red en internet", escrito por Alejandro Pisanty y Erik Huesca, se plantea un desafío desde lo técnico a la concepción política de neutralidad de la red de-

fendida alrededor del mundo. En el texto, los autores buscan aclarar los principios técnicos que rigen el funcionamiento de la red, incluyendo el trato sin discriminación, restricciones o interferencias de lo que transita por las redes. Sin embargo, para entender las implicaciones de este postulado en términos económicos y de derechos humanos, se debe dejar muy claro el funcionamiento de internet a nivel de protocolos, a salvo de los intereses comerciales de las empresas que operan en la red, pero también a salvo de los intereses estatales. Los autores ensayan así una dimensión distinta a una discusión compleja y altamente debatida.

Por último, Juan Manuel Casanueva escribe sobre "Gobierno abierto en el contexto mexicano" y las paradojas inherentes a este concepto. En 2015, la reunión anual de la Alianza para el Gobierno Abierto se llevó a cabo justamente en la Ciudad de México. La sociedad civil criticó fuertemente el evento, pues al mismo asistieron varios funcionarios públicos acusados de corrupción e inclusive se impidió el paso a diversas organizaciones de derechos humanos. Casanueva expone la paradoja mexicana: existen compromisos explícitos y resultados visibles en cuanto a los mecanismos de apertura de información, pero distintos gobiernos mexicanos no han dado muestras transversales de transparencia, apertura a la participación ni descenso de la corrupción. El cuestionamiento que subyace es cuánto aportan, entonces, las políticas de gobierno abierto a mejorar la transparencia y a hacer nuestros gobiernos más abiertos al control público.

En cada capítulo, cada autora y autor aportó una investigación

y un conocimiento invaluables tanto de las materias abordadas como de la realidad mexicana. La mezcla de derechos tan complejos y su ejercicio en un medio aún desafiante como internet, ameritan un profundo debate que permita robustecer los principios democráticos y el ejercicio de derechos fundamentales. Ese debate no comienza ni se agota con internet, pero propender a propuestas de prácticas y políticas públicas sobre la red desde los derechos, ayudará al desarrollo de los mismos hacia el futuro.

Con ese espíritu, buscamos entregar un aporte al contexto mexicano en la lucha por una internet abierta, libre, segura y plural. Un espacio en el que florezcan los derechos y no sobrevivan las amenazas. Un lugar de resistencia y de construcción de nuevos paradigmas. Un espacio para que los derechos fundamentales históricamente amenazados inicien un ciclo virtuoso hacia un pleno ejercicio. México es, sin duda alguna, un terreno fértil para ello.

Claudio Ruiz
Director ejecutivo
Derechos Digitales

En defensa del anonimato

Antonio Martínez Velázquez y José Flores Sosa

Who do you pretend to be when you go online by yourself?
How much opposite to you is the person you become?
Douglas Coupland, Hans Ulrich Obrist y
Shumon Basar, *The age of earthquakes*

Una de las discusiones recurrentes sobre el uso de internet es la transmisión de mensajes de forma anónima. El debate es relativamente reciente: el auge de las redes y medios sociales en la web ha añadido preguntas y preocupaciones, desde la idea que el anonimato fomenta actividades criminales, hasta que protegerlo vulnera la seguridad del resto de los usuarios.

Como han propuesto Doc Searls y David Weinberger en "World of Ends" (2003), internet no es una cosa, es un acuerdo que se da en dos niveles: por una parte, entre los transmisores de información a través del protocolo TCP/IP[1] y, por otra, entre sus usuarios. La información transmitida a través de la red es, en principio, anónima. Se trata, en esencia, de una red de confianza.

1 Esto es, el conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red.

Cada paquete de datos se transporta de un lugar a otro sin que su contenido sea conocido por los componentes de la red. Este mecanismo, propio del protocolo de internet (IP), ha permitido el crecimiento exponencial de la red como vía de comunicación. Los datos viajan de manera indiscriminada, sin importar si ellos corresponden a un correo electrónico, una fotografía o una canción. Si cada dato estuviera sujeto a revisión previa de su contenido o de su formato, internet no podría ser lo que es. Este principio de no discriminación de "paquetes de datos" de acuerdo a su naturaleza es lo que conocemos como neutralidad de la red.[2]

Lawrence Lessig (1999) señala que la identidad y la autenticación en internet son cuestiones diferentes. Debido a que las direcciones IP[3] no revelan información sobre qué datos son enviados o quién los envía –al menos no a simple vista– el sistema otorga, en principio, un carácter anónimo a esta transferencia. Las direcciones IP son virtuales y, como tales, no están necesariamente ligadas a una unidad en el mundo físico. Es decir, el anonimato de los datos está previsto ya en el diseño de la red.

No obstante, en la práctica, esto no implica que la identidad de los usuarios de internet esté completamente protegida. Si

2 El debate sobre la discriminación de los paquetes de datos de acuerdo a su naturaleza y cómo se transmiten a través de la red corresponde al debate sobre la neutralidad de la red, otra discusión actual sobre internet que se aborda en este libro.

3 Las etiquetas numéricas que identifican, de manera lógica y jerárquica, a la interfaz de una computadora dentro de una red.

bien la dirección IP no tiene una naturaleza vinculante con una persona, han existido intentos por forzar la relación entre datos y usuarios. Las demandas judiciales por violaciones de derechos de autor en internet, por ejemplo, asumen que hay un vínculo entre la dirección IP y el presunto infractor. Sin embargo, algunos de estos esfuerzos han sido desestimados a nivel judicial.[4]

Por otra parte, existe la percepción que internet es un espacio que, junto con posibilitar la creación de comunidades, por su naturaleza permite la "innovación sin permiso", con el cumplimiento de protocolos técnicos como única condición de participación en la red. Esta idea ha permitido la invención de distintos servicios para comunicarse en la red, desde los chats por terminal o IRC (protocolo de comunicación en tiempo real, a través de texto) hasta las aplicaciones de equipos móviles como Snapchat. La idea es acercar dos puntos de la red a través de la transmisión de datos inteligibles en nuestras pantallas.

Sin embargo, los usuarios y los aspectos técnicos de internet no son los únicos actores a considerar en el funcionamiento de la red; los Estados y las empresas privadas tam-

4 Así ocurrió, por ejemplo, en la decisión del juez Gary R. Brown en 2012 en una demanda masiva contra usuarios de BitTorrent. Raul y SJD, "New York judge blasts trolls' practices, recommends banning mass bittorent lawsuits in the district". *Fight Copyright Trolls*. 2 de mayo de 2012, http://fightcopyrighttrolls.com/2012/05/02/new-york-judge-blasts-trolls-practices-recommends-banning-mass-bittorent-lawsuits-in-the-district/ (consultado el 12 de octubre de 2015).

bién forman parte de esta compleja ecuación, cada uno en defensa de sus propios intereses, lo que con el transcurrir de los años se ha vuelto cada vez más notorio. En la interacción entre todos estos elementos –técnicos, humanos, legales, sociales, políticos– se genera la tensión respecto al anonimato en la red.

1. El lugar del anonimato: un territorio de paso

En un sentido estricto, difícilmente podríamos catalogar a internet como un "espacio" donde confluyen personas, ideas o negocios; esto porque lo que allí sucede carece de una expresión material concreta, y quienes lo ocupan, lo hacen desde un lugar distinto al de la materialidad tangible de internet (los cables, los enrutadores, los tubos).

Por sus características, internet es mejor entendido como un "no-lugar". Marc Augé (1992) se refiere a estos como espacios caracterizados por la soledad de los movimientos acelerados de los ciudadanos, que los usan como hilo de paso a alguna parte. Los no-lugares van en contra de cualquier idea de permanencia; son lugares de situaciones inestables y tránsito ininterrumpido: aeropuertos, estaciones de trenes, centrales de transferencia, así como las autopistas que hacen del territorio un lugar de paso.

Internet, como no-lugar, es uno de intercambio de datos. El valor se encuentra en la operación misma de transmitir y transportar datos –y con estos, información– a la mayor cantidad posible de personas; allí también se encuentra el valor económico de internet para las corporaciones que lu-

cran con esa información. De ahí que, aparentemente, sea de poca importancia la identidad de quienes intercambian estos paquetes de información.

Sin embargo, debe concederse que la economía en línea, si bien no se preocupa por la identificación específica del individuo, sí lo hace por la construcción de un perfil del consumidor, a partir de la recopilación masiva de datos del usuario de la red. Un ejemplo claro es el uso de *cookies*,[5] forma en que se recopila información relacionada con la actividad del usuario en su navegador y que posteriormente se envía a los sitios web. Estas *cookies* pueden incluir elementos que identifiquen a la persona (su correo electrónico, ubicación geográfica o hábitos de compra), aun sin haber solicitado su nombre o identidad legal.

1.1. Redefiniendo lo público

Sea considerado como lugar o no-lugar, ¿internet es un espacio público o privado? Para muchos analistas, la red se trata de "la nueva esfera pública". De acuerdo al sociólogo alemán Jürgen Habermas (1962), la esfera pública se encuentra:

> configurada por aquellos espacios de espontaneidad social libres tanto de las interferencias estatales como de las regulaciones del mercado y de los poderosos medios de comunicación. En estos espacios de discusión

5 Una *cookie* (o galleta informática) es un pequeño archivo con información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede conocer y consultar su actividad previa.

> y deliberación se hace uso público de la razón; de ahí surge la opinión pública en su fase informal, así como las organizaciones cívicas y, en general, todo aquello que desde fuera cuestiona, evalúa críticamente e influye en la política. En términos normativos, la publicidad[6] puede entenderse como aquel espacio de encuentro entre sujetos libres e iguales que argumentan y razonan en un proceso discursivo abierto dirigido al mutuo entendimiento.[7]

No todas las condiciones de la definición habermasiana son cumplidas a cabalidad en internet. En primer lugar, hace mucho que la red dejó de ser un espacio libre de la interferencia estatal o las regulaciones de mercado; por el contrario, estos dos agentes adquieren cada vez mayor poder dentro de las interacciones de la red. Lessig (1999) señala que la entrada del comercio incentivó cambios en la arquitectura de la red para proveer: 1) autenticación, para asegurar la identidad; 2) autorización, para asegurar que la persona realizara una determinada función; 3) privacidad, para evitar que otros pudieran ver los intercambios de datos; 4) integridad, para asegurar que la transmisión no fuera alterada en ruta; y 5) no repudiación, para asegurar que el emisor no pudiera negar que envió el mensaje.

En segundo lugar, la horizontalidad y la igualdad de condiciones en acceso y participación en internet se han ido de-

6 Entendida como "la cualidad o estado de público".

7 Juan Carlos Velasco. *Para leer a Habermas*. Madrid: Alianza Editorial, 2014, p. 170.

gradando constantemente; en buena parte, porque muchos servicios de internet han excluido –a través de sus políticas– a los individuos que por diversas razones han decidido comunicarse anónimamente o mediante el uso de seudónimos distintos de su nombre legal. La arquitectura actual de la red favorece que terceros funcionen como autoridades de certificación de la identidad, mediante sistemas que incentivan a los usuarios a identificarse voluntariamente.

Desde esta perspectiva, internet es una esfera privada que tiene consecuencias públicas. Esta naturaleza mixta impacta en la concepción y tratamiento del anonimato en línea. Se puede decir que, al tratarse de un espacio eminentemente privado, la expectativa de poder participar de forma anónima en la red es más alta que en los casos de publicidad o identificación pública obligada. No obstante, lo público –por su naturaleza– es altamente tolerante al anonimato: la identidad es la última opción de convivencia en un espacio de reglas claras. A buena parte de lo privado tampoco le importa mucho la identidad en sí misma (por ejemplo, en la compra tradicional en los supermercados) para sobrevivir.[8] Es en esta mezcla híbrida y acelerada en donde nuevas dinámicas complejas emergen e irrumpen el orden establecido.

Existe, sin embargo, una discrepancia respecto del trata-

8 Aunque, como se ha señalado con anterioridad, a lo privado puede interesarle la construcción de perfiles de usuario, que pese a no identificar puntualmente al individuo (o al menos, no siempre), sí lo relacionan con determinados rasgos demográficos y constituye un grado menor de identificación.

miento de la información por parte de los agentes privados. El hecho que los datos sean la moneda de cambio para el otorgamiento de servicios, modifica sustantivamente la relación entre las partes del contrato que el usuario "firma" a través de, por ejemplo, la aceptación tácita o expresa de los términos de servicio de las redes sociales. Es el usuario quien se encuentra en desventaja estructural frente a los dueños de los servicios, siendo despojado del control de sus datos al revelar su identidad.

Esta asimetría de poder pone al usuario común en una posición de vulnerabilidad dentro del contrato social en la red. Este estado de cosas tiene beneficiarios claros: por un lado, la industria de los intermediarios se beneficia de todo aquello que queda en la zona gris entre lo público y lo privado, y que en la práctica son tratadas como "cosas públicas" pero monetizadas como cosas privadas. Esta ambigüedad propicia la explotación de los datos sin el consentimiento o el conocimiento de los usuarios. Por otra parte, las empresas en internet se benefician del tratamiento de lo "público" como un estado binario porque el manejo de formas más complejas de privacidad puede ser más costoso de lo que están dispuestas a invertir en los intereses del usuario.

2. El anonimato como derecho

La capacidad de "ser anónimo" como derecho es una consecuencia del desarrollo de la libertad de expresión; reside en la voluntad de la persona para revelar o no uno de sus atributos personalísimos, la identidad, para establecer contacto con el mundo y para expresar sus ideas o acceder a información.

El anonimato permite que las personas establezcan códigos de comunicación para expresarse libremente. Estos códigos rompen los obstáculos que agentes externos imponen a la libre transmisión de ideas y opiniones. El anonimato se ha vuelto una forma de protección frente a posibles abusos, mientras que las políticas de revelación de identidad en la red afectan particularmente a grupos vulnerables y comunidades marginadas, como el caso de la política de nombres reales de Facebook y las personas transgénero (Kayyali, 2015).

La noción de anonimato como un derecho no es nueva. En diversos momentos de la historia latinoamericana se ha mantenido en reserva la identidad de las personas por motivos variados: la historia reciente de la región ha conocido distintos casos de dictaduras militares y gobiernos autoritarios que han perseguido a todo disidente, con métodos que incluyen los asesinatos masivos y las desapariciones forzadas; una realidad que, lamentablemente, también se ha vivido en México. La posibilidad de anonimato entre los disidentes se convierte en parte esencial de su derecho a expresarse y obtener información, disminuyendo el riesgo de persecución.

En muchos contextos, la condición de anonimato permite generar lazos de confianza entre los actores involucrados. Esto es especialmente importante en escenarios violentos en los que identificarse significa un riesgo y donde el anonimato permite brindar seguridad a los participantes de una conversación particular. Andrés Monroy-Hernández (Mustafaraj *et al.*, 2012) prueba cómo estas conexiones son importantes para la comunicación y coordinación de un grupo

social en condiciones vulnerables, mediante el ejemplo de la red #ReynosaFollow en Tamaulipas, un estado al norte de México dominado por el narcotráfico y en el que las balaceras callejeras son frecuentes y donde mediante la comunicación de mensajes al público, desde perfiles anónimos o no, identificados con la etiqueta #ReynosaFollow, se logra informar a la población general.

La seguridad de las comunicaciones en la red no está condicionada por la calidad de las personas ("identificadas" o anónimas), sino por la capacidad que tienen Estados, corporaciones y usuarios de acordar y mantener vínculos de confianza que promuevan la capacidad de ejercicio de la libertad de expresión, la diversidad de opiniones, la inclusión de los grupos marginados y reglas claras y transparentes de denuncia de conductas ilegales. El anonimato, en todas sus expresiones,[9] es un elemento que conlleva beneficios para una sociedad democrática al permitir la inclusión de voces vulnerables dentro de la deliberación pública.

3. La tensión entre la identidad real y el anonimato en internet

Aunque internet ensancha las capacidades formales y materiales para ejercer el derecho a la libre expresión, también ha ampliado las posibilidades para perseguir y censurar esa misma capacidad, a una escala quizás nunca imaginada. La era digital ha supuesto nuevos retos en el acercamiento del Estado, corporaciones y medios para entender la tensión en-

9 Incluyendo aquí desde el uso de seudónimos (para proteger la identidad de personas) hasta el cifrado de las comunicaciones (para proteger el contenido de las mismas, aun si los interlocutores no son anónimos).

tre la identidad real y el anonimato; es así que se encuentran al menos tres áreas del debate que han llevado a empresas y gobiernos a impulsar una agenda que privilegia una sobre la otra: la difamación, la vigilancia masiva y la dinámica del comercio en línea.

3.1 La difamación y el derecho al honor

Existe un aparente conflicto entre el derecho a la libertad de expresión y los llamados "delitos contra el honor": calumnias, difamación e injurias. El anonimato guarda una relación con esa tensión, porque garantiza que quien emite el mensaje no sea víctima de represalias en caso de exposición o denuncia (permitiendo así una expresión más libre), mientras que quienes pretenden castigar este tipo de mensajes recurren al argumento de la identidad real para buscar reparación o inhibir este tipo de acciones.

Si bien algunas de las ofensas son "reparables" mediante rectificaciones, disculpas o réplicas –además de la compensación monetaria– en la práctica, la tensión se encuentra en la difusa definición de lo que constituye una difamación. La intimización de lo público y la publicidad de lo privado que ha generado la arquitectura de la red, rompen el paradigma de una nítida separación entre ambos mundos, de modo que la laxa interpretación acerca de lo ofensivo conlleva un riesgo para quienes ejercen opiniones "incómodas" hacia personajes como políticos, funcionarios o cualquier individuo con poder.

Es por ello que algunos delitos contra el honor han sido

proscritos en muchos estados y también a nivel federal, y por lo cual el Comité de Derechos Humanos de la ONU ha recomendado la despenalización en los estados restantes[10]: para evitar que la protección del derecho al honor llegue a tal punto que quede por encima del derecho a la libertad de expresión.

Tradicionalmente, en los medios analógicos, la respuesta a un contenido difamatorio debe pasar por editores de tales medios para poder manifestarse, conforme a las limitaciones de la comunicación pública por canales controlados como la prensa y la radiodifusión. En internet la posibilidad de contestación es instantánea y la falta de filtros permite combatir la difamación: una réplica no necesariamente debe pasar por un intermediario, sino que puede llegar directamente con el interlocutor. No obstante, Estados y corporaciones han intentado regular estos procesos de autogestión por la vía de la criminalización de contenidos a nivel del intermediario o de quien facilita la expresión.

Ninguno de los servicios de internet ha ofrecido soluciones claras a posibles casos de censura colectiva, que puedan ser replicados o convertidos en estándar. Esto se debe al irreductible conflicto entre la tradición jurídica europea y la estadounidense en el tratamiento de la libertad de expresión (y las soluciones que ambas alternativas suponen), aunado

10 Comité de Derechos Humanos de Naciones Unidas, Observaciones finales del Comité de Derechos Humanos, Examen de los informes presentados por los Estados partes en virtud del artículo 40 del Pacto, México, CCPR/C/MEX/CO/5, 7 de abril de 2010.

al nuevo papel de los particulares –los dueños de los grandes concentradores de la expresión en la red: Facebook, Twitter y Google– como censores privados de sus comunidades; una monarquía digital.

De la tradición europea se desprende, por ejemplo, la teoría del honor colectivo: el reconocimiento explícito de que no solo los individuos, sino también los grupos sociales (con sus características y atributos específicos), tienen un honor que el Estado debe proteger a partir de la modulación del lenguaje en lo público. Así es posible garantizar que todos se expresen en igualdad de condiciones y que el Estado brinde ventajas (vía la protección) a quien se encuentra en desventaja estructural.

Por su parte, la tradición jurídica estadounidense ha reforzado el poder de la Primera Enmienda de su Constitución desde la posguerra. Por esa razón, su sistema parece desfasado del resto, ya que no pondera de manera equilibrada los derechos frente a la libertad de expresión, sino que asigna a esta un valor superlativo. A diferencia de la tradición europea, Estados Unidos protege prácticamente cualquier discurso en la conversación pública, desde voces segregadas hasta las radicales y, por supuesto, las anónimas.[11]

11 American Civil Liberties Union, "In Two Significant Cases, ACLU Seeks to Protect Anonymous Online Speakers From Legal Intimidation". ACLU, 26 de febrero de 2001, https://www.aclu.org/news/two-significant-cases-aclu-seeks-protect-anonymous-online-speakers-legal-intimidation (consultado el 15 de octubre de 2015).

Desde esta perspectiva, ningún derecho parece posible sin que la libertad de expresión esté garantizada casi en términos absolutos. El siguiente texto de la Unión Estadounidense por las Libertades Civiles (ACLU) es ilustrativo:

> La ACLU ha estado a menudo en el centro de la controversia por defender la libertad de expresión de grupos de odio, tales como el Ku Klux Klan y los Nazis. Pero si solo las ideas populares fueran protegidas, no necesitaríamos una Primera Enmienda. La historia nos muestra que el primer blanco de la represión gubernamental nunca es el último. Si no defendemos los derechos a la libertad de expresión de los menos populares entre nosotros, incluso si sus puntos de vista son antitéticos a los de la misma libertad que la Primera Enmienda defiende, entonces la libertad de nadie estará segura. Censurar el llamado discurso de odio también contrarresta los intereses a largo plazo de las víctimas más frecuentes de odio: minorías raciales, étnicas, religiosas y sexuales. No debemos dar al gobierno el poder de decidir qué opciones son de odio, ya que la historia nos ha enseñado que el gobierno es más apto para usar ese poder para perseguir minorías en vez de protegerlas.[12]

John Stuart Mill (1859) planteó la regulación del discurso como el libre mercado, de manera que todas las expresiones tienen cabida, porque el Estado ha creado un campo igua-

12 American Civil Liberties Union, "The First Amendment Ignored", ACLU, https://www.aclu.org/freedom-expression-0#3 (consultado el 15 de octubre de 2015). Traducción de los autores.

litario para que cada uno pueda expresarse. En contraste a los europeos, no se analiza el contenido del discurso y sus consecuencias, sino la capacidad para ejercerlo. Se garantiza la libertad de expresión y, en la lógica de mercado, los peores discursos acaban por salir de la conversación pública sin necesidad de proscribirlos.

Por tanto, se puede ver cómo se perfilan dos visiones claramente contrapuestas: la del Estado como curador del discurso, en tanto depositario de la voluntad social, y la del Estado como mero guardián del espacio público para expresarse en libertad y autorregularse. Ambas visiones comparten la finalidad que la sociedad evolucione en su capacidad de entendimiento; sin embargo, las vías utilizadas (y probablemente los resultados) son distintos. El dilema se encuentra entre un Estado que conoce y evalúa el contenido de las manifestaciones para prevenir consecuencias públicas indeseables y un Estado al que no le interesa el contenido sino la capacidad de ejercicio.

En internet, los servicios intermediarios de la expresión han optado –indistintamente de su país de origen– por ambas visiones o por una combinación de ellas, como en el caso de Facebook tomando partido por la censura de ciertos discursos por ofensivos o chocantes. En este sentido, prohibiciones como la muestra de pezones femeninos en imágenes publicadas en la red social hacen evidentes los problemas de esta perspectiva híbrida, en la que los criterios para regular (o intentar regular) el discurso terminan por censurar expresiones artísticas, sociales y culturales legítimas.

Al respecto, la política de desnudos en las normas comunitarias de Facebook[13] dice:

> Restringimos la exhibición de desnudos para evitar que determinados sectores de nuestra comunidad mundial que muestran una especial sensibilidad ante ellos se puedan sentir mal, en particular, por su contexto cultural o su edad (...) Como resultado, nuestras políticas pueden ser a veces más directas de lo que nos gustaría y restringir contenido compartido con fines legítimos (...) Eliminamos fotografías que muestren los genitales o las nalgas en su totalidad y de una forma directa. También restringimos algunas imágenes de senos femeninos si se muestra el pezón, pero siempre permitimos fotos de mujeres amamantando o que muestren los pechos con cicatrices por una mastectomía. También permitimos fotografías de pinturas, esculturas y otras obras de arte donde se muestren figuras desnudas. Las restricciones sobre la exhibición de desnudos y actividades sexuales también se aplican al contenido digital, a menos que dicho contenido se publique con fines educativos, humorísticos o satíricos. Se prohíben las imágenes explícitas de relaciones sexuales. También podemos eliminar descripciones de actos sexuales que sean demasiado gráficas.[14]

13 Al 15 de octubre de 2015. Las normas comunitarias de Facebook cambian regularmente.

14 Facebook, "Normas comunitarias". Publicado el 16 de marzo de 2015 https://www.facebook.com/communitystandards (consultado el 15 de octubre de 2015).

En contraste, Facebook se convierte en blanco de crítica al erigirse como un juez de las expresiones, siendo constantemente apuntado por su permisividad hacia el discurso de odio o los mensajes racistas y/o xenófobos. Incluso la Canciller alemana, Angela Merkel, criticó duramente a Mark Zuckerberg durante una reunión en la Organización de las Naciones Unidas por "bajar rápidamente fotografías consideradas indecentes mientras que fallaba en mantener su política sobre discurso de odio" (citada en Porter, 2015).

Son justo regulaciones de este tipo las que atentan contra el anonimato, en tanto pretenden servir como justificación para controlar el discurso. La política de discurso de odio[15] de Facebook también es empleada como justificación para su política de identidad real al señalar que:

> Permitimos comentarios humorísticos o satíricos relacionados con estos temas y creemos que, cuando la gente usa su identidad real, es más responsable a la hora de compartir este tipo de comentarios. Por este motivo, pedimos a los propietarios de las páginas que asocien su nombre y perfil de Facebook a cualquier contenido que sea insensible, incluso si ese contenido no infringe nuestras políticas. Como siempre, instamos a las personas a ser conscientes de su público cuando compartan este tipo de contenido.

15 Facebook cuenta con un apartado sobre discurso de odio en sus normas comunitarias, en el que indica que "no admite organizaciones ni personas dedicadas a promover el odio hacia estos grupos protegidos en su plataforma".

De este modo, es evidente cómo la política de identidad real de Facebook entra en tensión con la libertad de expresión mediante la prohibición directa y táctica del anonimato, como consecuencia de esta hibridación a conveniencia de las normas para combatir la difamación. Aunque Facebook parece tener conciencia de la problemática que aborda ("nuestras políticas pueden ser a veces más directas de lo que nos gustaría y restringir contenido compartido con fines legítimos"),[16] sus políticas favorecen la anulación del anonimato bajo supuestos ("creemos que, cuando la gente usa su identidad real, es más responsable a la hora de compartir este tipo de comentarios"), lo que termina por lesionar los derechos de terceros, especialmente de grupos vulnerables (Kayyali, 2005).

3.2. La vigilancia masiva contra el anonimato en internet

Una segunda gran área de riesgo para el anonimato en línea es la vigilancia masiva. Los Estados han aprovechado la concentración de servicios de telecomunicaciones, operadores, proveedores de servicios de internet y proveedores de servicios web (por ejemplo, Google o Facebook), de manera tal que pueden desarrollar con más facilidad la vigilancia de las comunicaciones que se sirven de esos servicios, con concurrencia entre estas corporaciones y el gobierno. Los Estados han encontrado la manera de intervenir todas las

16 Facebook ha modificado sus normas por presión social, como muestra la aclaración "pero siempre permitimos fotos (...) que muestren los pechos con cicatrices por una mastectomía". Dicha enmienda fue hecha en 2013 como resultado de una petición con más de 20 mil firmas en Change.org. Véase Susan Donaldson James, 2013.

comunicaciones y datos generados en los espacios digitales para construir la herramienta de vigilancia más poderosa de la humanidad, con información provista muchas veces por los mismos usuarios. Señala Jéremie Zimmermann:

> No es solo la vigilancia financiada por los Estados, es la cuestión de la privacidad; la forma en que la información está siendo manejada por terceros y el conocimiento que la gente tiene sobre lo que se está haciendo con dicha información (...) Facebook hace negocio difuminando esta línea entre lo privado, los amigos y la publicidad, e incluso está almacenando información en principio destinada únicamente a tus amigos y seres queridos.[17]

Asimismo, la recopilación de metadatos –o "datos sobre los datos"–[18] de correo electrónico, ubicación, búsquedas y visitas revelan tanto más de las personas que los contenidos por sí mismos; como indicó Stewart Baker, ex consejero general de la Agencia de Seguridad Nacional de Estados Unidos (NSA), "los metadatos dicen todo sobre la vida de alguien (...) si tienes suficientes metadatos no necesitas realmente

17 Citado en Julian Assange *et al., Cypherpunks: La libertad y el futuro de Internet* . México, DF: Planeta, 2012.

18 El término metadatos se refiere a "datos altamente estructurados que describen información, describen el contenido, la calidad, la condición y otras características de los datos". Es "información sobre información" o "datos sobre los datos". Véase "Metadatos" en Sistema de Información de la Amazonia Colombiana, Universidad Nacional de Colombia, sede Amazonia, http://www.unal.edu.co/siamac/sig/metadatos1.html (consultado el 15 de octubre de 2015).

contenidos (…) Es algo embarazoso cuán predecibles somos como seres humanos" (citado en Rusbridger, 2013). El trazo de ciertos patrones en control del Estado puede producir abusos constantes de la ley.

La vigilancia masiva pone en entredicho el derecho de las personas a protegerse a sí mismas, su derecho a mantener una forma de control sobre sus datos –entre ellos, su identidad– por razones de seguridad. Prácticas como el cifrado de las comunicaciones permite que el usuario pueda guardar anonimato sobre su información, así como el uso de redes de enrutado anónimo como Tor le facultan para ocultar su ubicación de terceros; ambas herramientas son cruciales para personas en profesiones o situaciones de alto riesgo, como periodistas, activistas, defensores de derechos humanos e informantes, entre otros.[19]

Por tanto, si las empresas como Facebook y Google están realmente comprometidas con la seguridad de sus usuarios, ¿qué necesitan para tomarse en serio el tema? No todo el mundo está más seguro por dar su nombre real. Al contrario: muchas personas están mucho menos seguras cuando son identificables y quienes están menos seguros son, a menudo, los más vulnerables.

El caso de la periodista estadounidense La Gringa es ilustrativo. La Gringa es una bloguera que usaba su seudónimo

19 "Inception". Tor Project. https://www.torproject.org/about/torusers.html.en (consultado el 16 de octubre de 2015).

para reportar el crimen en Honduras, hasta que Facebook suspendió su cuenta por no utilizar su nombre real (Heim, 2011). La Gringa criticó la decisión de Facebook en su blog, recordando que Honduras estaba clasificado en 2010 por Reporteros Sin Fronteras en el lugar 143 de 178 países para ejercer el periodismo.

Al respecto, Rebecca McKinnon menciona que:

> Los reyes soberanos de Facebookistán refuerzan esta política de la "identidad real". Cuando son descubiertas, las cuentas que usan seudónimos o identidades falsas son castigadas con la suspensión de la cuenta o la desactivación. Este sistema de gobernanza interna trasciende naciones físicas, a través de democracias y dictaduras. Influye en la habilidad de la gente para comunicarse no solo a través de Facebook mismo, sino también a través de un universo expandiéndose rápidamente de otros sitios web y servicios que están integrados cada vez más con Facebook.[20]

La vigilancia masiva no solamente afecta de manera directa la privacidad de las personas. Quizá el efecto más grave está en la capacidad de la vigilancia para inhibir la libertad de expresión. El comportamiento del ser humano se ve modificado ante la mera noción de saberse vigilado, lo que difumina también la esfera privada. Las consecuencias de este panóptico limitan la manifestación de ideas, incluso en los espacios más íntimos. Los límites de lo público deben ser

20 McKinnon, Consent of the Networked: The Worldwide Struggle For internet Freedom. Nueva York: Basic Books, 2013. [Traducción de los autores]

reimaginados, siempre en beneficio –y no en perjuicio– de los menos protegidos.

3.3. El anonimato en la economía en línea

Una tercera cuestión que amenaza al anonimato obedece a las dinámicas de la economía en línea. Ante el riesgo de una posible suplantación de identidad –con las consecuencias que esto conlleva para las víctimas de fraude y para las propias empresas– las entidades bancarias y comerciales han privilegiado la identidad como un mecanismo de seguridad. El usuario queda obligado a autenticarse para poder hacer uso de una gran cantidad de servicios financieros en la red, de modo que el prestador tenga la mayor certeza posible de estar entregando la información a la persona correcta.

Lessig (1999) recuerda que internet no fue concebido originalmente para el comercio, sino para la investigación. Fue la entrada del comercio lo que impulsó cambios en la arquitectura de la red: "Al inicio, los vendedores estaban bastante ansiosos acerca de las transacciones en línea; las compañías de tarjetas de crédito inicialmente no querían que sus números se usasen en el ciberespacio; al menos, no hasta que el ciberespacio cambió".

¿Están los servicios en línea terminando con la posibilidad de una transacción anónima? Actualmente, este atributo se manifiesta cada vez con mayor frecuencia en servicios de comercio en línea, especialmente dentro de la economía colaborativa, que se basa fuertemente en la reputación del proveedor. Casos como Uber o Airbnb requieren que los usuarios,

prestadores del servicio o consumidores, hagan pública su identidad como un indicativo de certidumbre. Por ejemplo, el servicio de renta colaborativa Airbnb solicita durante el registro que el usuario digitalice un documento de identidad oficial –como un pasaporte– como requisito de uso.[21]

Son cada vez menos comunes los servicios de transacciones en línea que no requieren al usuario autenticar su identidad legal. Eso se debe a diferentes condiciones relacionadas con la seguridad; por ejemplo, en el caso de PayPal, con las políticas de diferentes naciones en contra de la evasión fiscal o del lavado de dinero; mientras que con Airbnb o Uber, con cuestiones relacionadas con el cobro de seguros o la reparación de daños a terceros.

Sin embargo, esta práctica también está acompañada de la explotación de los datos de los usuarios. Como expone Richard Stallman (2014) en su crítica a Uber, el taxi tradicional es anónimo: se paga el viaje y se llega al trayecto sin que el conductor conozca nuestra identidad. En contraste, el usuario de Uber permite a la aplicación el acceso a ubicación geográfica, información de contactos, mensajes de texto y páginas visitadas, entre otros.[22] La empresa también ha sido

21 "¿En qué consiste el proceso de Identificación verificada?", Airbnb, https://www.airbnb.mx/help/article/450/what-is-verified-id (consultado el 16 de octubre de 2015).

22 "Datos personales corren riesgo en manos de Uber: especialista". *El Universal,* 3 de julio de 2015., http://archivo.eluniversal.com.mx/periodismo-datos/2015/datos-personales-corren-riesgo-uber-107923.html (consultado el 16 de octubre de 2015).

acusada de permitir a sus empleados acceso sin restricciones a la información personal de los usuarios, incluido el rastreo en tiempo real de sus recorridos (Mueffelmann, 2015).

Así, el uso de los datos como moneda de cambio representa un riesgo latente para la privacidad; mucho más en una economía en línea que restringe el anonimato bajo un argumento de confiabilidad en la transacción. Esto, sumado a la vigilancia masiva, tiene impacto directo en las libertades, como ejemplifica Jacob Applebaum:

> No podemos afirmar que el sistema económico habita en una especie de vacío. El sistema de comunicación está directamente vinculado a ello (...) Ni siquiera es posible comprar un boleto de avión sin una moneda rastreable. Estás fichado. Y si decides dirigirte a un aeropuerto y, pagando en efectivo, tratas de comprar un boleto para ese mismo día, te fichan. Te aplican medidas extraordinarias de seguridad. No puedes volar sin identificación y, si tuvieras la mala suerte de haber comprado tu boleto de avión con una tarjeta de crédito, registran todos tus datos, desde tu dirección IP hasta tu navegador.[23]

4. Defender el anonimato

Los argumentos en contra del anonimato en la red, tanto por legisladores, políticos y empresarios, radican en promover políticas de "identidades reales", declarando dos fines específicos: 1) elevar la calidad de la conversación y 2) aumentar la seguridad de los usuarios en línea.

23 Citado en Assange *et al.*, obra citada.

Ninguna de las dos resultados se obtiene a cabalidad por la sola identificación de las personas. Basta pensar "¿cómo es una conversación de 'nivel elevado'?" La respuesta dependerá de la posición que ocupe quien responda. Internet es una fuente casi inagotable de información y datos. A diferencia de la era dominada por los periódicos impresos y la televisión, en la que la opinión publicada se encontraba mediada y editada, en la que la información era escasa y se requería "tener un nombre" para poder opinar públicamente, en la era digital el paradigma se ha subvertido. No existe, por lo menos formalmente, esa barrera que media la opinión publicada.

La construcción de la identidad en línea no se encuentra determinada por sus elementos jurídicos o materiales, sino que parte de la expresión de la voluntad personal. En este sentido, el paradigma de la identidad se ha vuelto flexible y líquido para ajustarse a los deseos de la persona que logra deshacerse de barreras impuestas en su construcción identitaria. Pero además, desde una perspectiva ontológica, esto permite que la persona construya una identidad en la red que trasciende los rasgos "definitorios" del ser, abriéndole un espectro de posibilidades para experimentar –aunque sea de manera velada– otros aspectos de su personalidad que, de otra manera, sería incapaz de ejercer. En la historia de internet, espacios como los juegos de rol en línea (MMMORPG) o los foros de discusión, han permitido la construcción de identidades alternas que permiten al individuo transgredir y trascender características personales como el género, la edad y la apariencia física.

El anonimato es, en este sentido, una expresión más de la identidad de la persona; una en la que puede explorar facetas o realizar acciones que de otra manera serían imposibles o muy difíciles. Desde la denuncia de abusos, como en el caso de los informantes o *whistleblowers*, hasta la expresión y goce de una identidad sexogenérica, los casos en los que el anonimato incentiva las libertades del ser son vastos y deben ser protegidos. De allí que en la red el código entre usuarios, los elementos objetivos de legitimidad, veracidad, interés y "voz" no están ligados a la identidad jurídica y formal de las personas sino a construcciones comunitarias que validan la identidad de cada usuario preservando el protocolo de confianza.

Un claro ejemplo de esto se encuentra en el Movimiento Zapatista en México de 1994.[24] El uso deliberado del anonimato (mediante los pasamontañas y los seudónimos) no interrumpió en absoluto las negociaciones de paz con el gobierno, ni el mensaje central de colocar la autonomía y dignidad de los pueblos originarios en el centro de la discusión pública. De la misma forma, la calidad de las conversaciones en línea no se encuentra atada a la identidad de sus usuarios sino al fondo mismo de los asuntos.

Mario Tascón y Yolanda Quintana Serrano, autores de *Ciberactivismo: las nuevas revoluciones de las multitudes conectadas*,

24 El término zapatista se utiliza indistintamente para referirse al movimiento agrarista liderado por Emiliano Zapata a principios del siglo XX y al levantamiento campesino del estado mexicano de Chiapas en 1994, liderado por el Ejército Nacional de Liberación Nacional (EZLN).

escriben en el diario español *El País* al respecto de la estrategia de anonimato zapatista:

> La comunicación de guerrilla centra buena parte de su estrategia en la batalla en torno a los símbolos. Y ahí el pasamontañas de Marcos, igual que en la actualidad la máscara de Guy Fawkes, anticipaba la reinterpretación del liderazgo de las nuevas revoluciones, en las que los perfiles individuales se difuminan en una identidad colectiva. Una idea que puede resumirse en la frase del Subcomandante: "detrás de nosotros estamos ustedes". O, de forma más directa, cuando escribieron: "Marcos es un ser humano, cualquiera, en este mundo. Marcos es todas las minorías intoleradas, oprimidas, resistiendo, explotando, diciendo: ¡Ya basta!" El pasamontañas, el nombre irreal o la ausencia de biografía de su portavoz no hacían sino evocar al "todos", del mismo modo que el colectivo Anonymous apela al 99%.[25]

La dinámica de lo anónimo también permite una reconfiguración sobre qué consideramos relevante en un contexto o entorno determinado. El anonimato también libra de ciertos juicios –considérese, por ejemplo, un concurso en el que los autores remiten bajo seudónimo para ser calificados por su obra– y permite ejercicios democráticos, como el secreto del

25 Mario Tascóny Yolanda Quintana Serrano, "Del pasamontañas a la máscara", *El País*, 23 de enero de 2014, http://elpais.com/elpais/2014/01/22/opinion/1390422170_938611.html (consultado el 16 de octubre de 2015).

voto, que resguardan la seguridad y la integridad de quienes participan de ellos.

Por ejemplo, en la edición 2015 de Wikimania, el fundador de Wikipedia, Jimmy Wales, otorgó por primera vez el premio de Wikipedista del Año *in pectore*; es decir, sin revelar la identidad del ganador de forma pública para proteger su identidad de represalias de carácter político.[26]

Así, el argumento de la calidad de la conversación ha sido utilizado también por su vinculación con el derecho al honor. Nuevamente, el problema radica en la confrontación que existe entre las tradiciones occidentales. Muchos sitios web han optado por incluir sistemas de autenticación de identidad para quienes comentan (algunos, basados en Facebook, convertido hoy en día en una especie de tarjeta de identidad de facto), de modo que quien se expresa pueda ser, de algún modo, auditable sobre las consecuencias de sus palabras. Es claro que esta decisión se ha tomado con la finalidad de reducir los insultos, los ataques y las expresiones de odio, pero también pueden inhibir otros discursos de personas que no desean ser identificadas.

Respecto al problema de seguridad de los usuarios, las categorías que suelen usarse son parcialmente verdaderas. Una de las más recurridas es la de utilidad pública de la identidad

26 Joe Sutherland, J, "2015 Wikipedians of the Year unveiled in Mexico". *Wikimedia Blog,* 31 de julio de 2015, https://blog.wikimedia.org/2015/07/31/wikipedians-of-the-year-2015/ (consultado el 15 de octubre de 2015).

para asegurar confianza del resto. El problema radica en que no todos pueden o quieren usar su identidad real y que la utilidad pública de hacerlo en la red no afecta la seguridad de terceros. Un usuario que logra poseer control sobre su identidad tiene mayores capacidades de participación en la red que aquel que ha sido despojado de ese control.

Sin embargo, para el discurso del Estado, el argumento de la seguridad pasa por la capacidad que tiene de identificar a una persona en caso de deslindar responsabilidades. Pero esta aproximación tienen un carácter erróneo, una suposición previa de que todos los ciudadanos son criminales en potencia. La identificación del infractor se busca hacer *ex ante,* lo que provoca un sistema de ideales de impartición de justicia que terminan por justificar, en el ideario político y en la opinión pública, la noción de que la identificación previa es el seguro en el que debe basarse la confianza en las instituciones.

La propuesta de criminalización de los encapuchados (personas que cubren su rostro con capuchas, máscaras, pasamontañas u otras prendas) en México en 2013, es una muestra de lo anterior:

> El 21 de marzo de 2013, el diputado Jorge Francisco Sotomayor Chávez del Grupo Parlamentario del Partido Acción Nacional (...) propuso penas de 10 a 20 años de prisión, y suspensión de los derechos políticos hasta por 10 años, a quien realice actos contra las personas, las cosas, servicios públicos o privados que "perturben la coexistencia pacífica, armónica y civilizada" de los ciudadanos. Para rematar –según la iniciativa– las penas

> se agravarían para aquellas personas que actúen encapuchadas (...) un ciudadano puede manifestarse con o sin ropa, en botarga o con la cara lavada, pero el derecho a mantener el anonimato dentro de una marcha con tintes políticos existe. No sería la primera vez que los individuos que se manifiesten públicamente sean fotografiados, fichados y posteriormente amenazados por órdenes de ciertos gobernantes en desacuerdo con manifestaciones en su contra. No existen disposiciones legales que limiten las capacidades de investigación del gobierno, especialmente sobre lo que ocurre en la vía pública. Todo acto ilícito debe ser castigado independientemente de la vestimenta que se use.[27]

El anonimato y la protección de la privacidad garantizan la no intromisión de terceros agentes en la información personal de los usuarios. Así, las personas que utilizan internet a través de espacios de anonimato no necesariamente se encuentran más vulnerables que aquellos confinados a los espacios "seguros" de las identidades reales. La relación entre la identidad real y una mayor seguridad para el usuario es, muy a menudo, artificiosa.

Por el contrario: los ambientes de identidades reales conllevan por sí mismos vulnerabilidades básicas; a saber, la posibilidad de robo de identidad, el uso indebido de datos personales, el acoso cibernético, el fraude económico y la persecución gu-

27 "Comunicado. La protesta no es violencia". Artículo 19, 25 de junio de 2013, http://articulo19.org/comunicado-la-protesta-no-es-violencia/ (consultado el 15 de octubre de 2015).

bernamental. En Estados Unidos, un caso de Facebook y las supervivientes de violencia doméstica evoca una de las peores facetas de la política de identidad real: una mujer que se había ocultado de su ex marido fue hallada por él justamente porque Facebook la orilló a usar nuevamente su identidad legal. Estuvo 18 años protegiéndose mediante seudónimos de un hombre que casi la mata; con el cambio, a su atacante solo le tomó dos semanas hallarla. Como señala Sarah Rogers "para sobrevivientes como Lily, un seudónimo no es una capa para comportamiento agresivo: es un escudo".[28]

5. Recomendaciones

El anonimato en línea debe protegerse por todos los actores involucrados en la gestión de internet. En una red libre, diversa y democrática, los usuarios deben tener la posibilidad de identificarse con los elementos que más se ajusten a su persona y los servicios en la web no deberían sancionar a quien así lo decida.

Las políticas referentes a las "identidades reales" son un abuso de poder. Este tipo de políticas vulnera el derecho de las minorías y los grupos marginales para expresarse de manera libre, además de atentar contra el derecho a la privacidad de los datos de las personas: entre más datos expuestos, más probable será que los instrumentos de vigilancia masiva tengan control sobre sus identidades.

28 Sarah Rogers, "How Facebook Exposes Domestic Violence Survivors", *The Daily Beast*, 20 de mayo de 2015, http://www.thedailybeast.com/articles/2015/05/20/how-facebook-exposes-domestic-violence-survivors.html (consultado el 15 de octubre de 2015).

El Estado debe dejar de pensar en el anonimato como un encubrimiento de lo ilícito y considerarlo como parte fundamental del derecho a la libertad de la expresión. La asociación peyorativa de lo anónimo con lo criminal se da en países donde el disenso es incómodo, como el caso expuesto sobre los encapuchados en la protesta en México.[29]

Es comprensible que el Estado utilice la identidad como un mecanismo de protección, como en las transacciones en línea o para la identificación de conductas ilegales; sin embargo, esto nunca debe hacerse para justificar medidas que vulneren los derechos fundamentales o pongan en riesgo la privacidad de los ciudadanos, como la recolección masiva e indiscriminada de datos, la geolocalización en tiempo real sin orden judicial o las leyes que promuevan la censura previa o incentiven a intermediarios a aplicar la remoción de contenidos.

El Estado debe garantizar que los grupos vulnerables tengan acceso al anonimato, generando mecanismos de protección que aseguren que no sufran consecuencias indeseables. Para ello, la aplicación del principio de proporcionalidad es indispensable, entendiendo, en palabras de Julian Assange, que se debe asegurar la privacidad para el débil y transparencia para el poderoso.[30] La identificación del individuo debe darse en casos específicos y no como una norma, permitiendo que la persona pueda reservarse el derecho a hacer público uno, alguno o todos los rasgos que le identifiquen jurídicamente.

29 Véase Artículo 19, obra citada.

30 Véase Assange (2012), obra citada.

Es tentador para los Estados caer en la creación de políticas que apuntan hacia el lado opuesto, debido a que aparentan beneficios sobre la seguridad pública. Ese es el argumento de la vigilancia masiva, que crea el riesgo de la elaboración de perfiles previos y, en el caso de sociedades con debilidad institucional, el espionaje de grupos incómodos al poder como, periodistas, activistas y defensores de derechos humanos, entre otros. En sociedades de este tipo, donde la corrupción y el abuso son cotidianos, es imperativa la protección del anonimato para permitir la libre expresión, la libre asociación y la manifestación de ideas.

El Estado no debe restringir las posibilidades legales ni técnicas para el discurso anónimo y las herramientas de ocultación de identidad. El reciente reporte del relator especial de la ONU para la protección de la libertad de expresión, David Kaye, establece que:

> Los Estados no deben restringir el cifrado y el anonimato, que facilita y a menudo hace posible el derecho a la libertad de opinión y expresión. La prohibición general falla en ser necesaria y proporcionada. Los Estados deben evitar todas las medidas que debiliten la seguridad que los individuos deben gozar en línea, como las puertas traseras, estándares débiles de cifrado y la retención de claves por parte de terceros. Adicionalmente, los Estados deben abstenerse de hacer que la identificación de usuarios sea una condición para el acceso a las comunicaciones digitales y servicios en línea, y requerir el registro de tarjetas SIM para el registro de usuarios móviles.

> Los actores corporativos deben asimismo considerar sus propias políticas que restrinjan el cifrado y el anonimato (incluido a través del uso de seudónimos). El descifrado ordenado por la corte, sujeto a las leyes nacionales e internacionales, debe ser permisible solamente cuando resulte de leyes transparentes y públicamente accesibles aplicadas solo a individuos (es decir, no a un grupo de personas) con un fundamento dirigido caso por caso y sujeto de una orden judicial y a la protección del derecho al debido proceso de los individuos.[31]

Los intermediarios no quedan exentos de estas responsabilidades. Así como los Estados deben evitar leyes que fuercen a estos actores a acatar consecuencias por la libre expresión de sus usuarios (por ejemplo, sitios que son cerrados por infracciones de propiedad intelectual de terceros distintos al titular), es deber de las empresas oponerse en los tribunales a este tipo de medidas coercitivas.

Pero, sobre todo, el Estado es quien debe ser garante del anonimato para terceros, pero no escudarse en él. El anonimato es asimétrico respecto al poder: lo equilibra cuando está del lado del vulnerable, lo acentúa cuando es empleado por el poderoso. La opacidad gubernamental, la secrecía y el ocultamiento son manifestaciones que propician el abuso, la impunidad y limitan la rendición de cuentas.

31 Oficina del Alto Comisionado de Naciones Unidas para Derechos Humanos, *Report on encryption, anonymity, and the human rights framework*, 19 de junio de 2015, www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (consultado el 17 de octubre de 2015)

Por supuesto que existen condiciones de abuso del anonimato –el acoso sexual, el fraude–, pero se dan en condiciones donde quien lo ejerce busca aumentar la brecha en su relación de poder respecto al afectado. Es en estos casos en los que, tal como señala Kaye, se debe contar con mecanismos de identificación y descifrado que sean individuales (jamás masivos), aplicados bajo las condiciones específicas de cada caso, respetuosos de los derechos humanos y siguiendo el debido proceso.

¿Cuál es el fin de penalizar o proteger el anonimato en línea? Aunque encontradas, las dos posturas parecen tener un mismo fin: una red más armónica para la convivencia y confiable para el intercambio de información. Hoy, los *trolls* o los *bots* son los que suelen ocupar las páginas de los medios para recordarnos los problemas que acarrea una red donde se permite el anonimato. Sin embargo, esta discusión está desbalanceada. La defensa del anonimato se vuelve esencial cuando se trata de asegurar voz a los excluidos. Las desigualdades de acceso a voz pública por cuestiones políticas, raciales, de clase o género, se replican y magnifican en la red. Cada política pública tendiente a prohibir el anonimato en línea debería ponderar desde esta óptica. Un *troll* menos no vale una vida más.

Augé, Marc. *Los no lugares, espacios de anonimato. Antropología sobre modernidad.* Barcelona: Gedisa, 1992.

James, Susan Donaldson. "Facebook Allows Mastectomy Photos, Not Nudity", *ABC News*, 12 de junio de 2013. http://abcnews.go.com/blogs/health/2013/06/12/facebook-launches-new-policy-to-allow-mastectomy-photos/ (consultado el 15 de octubre de 2015).

Heim, Anna. "How Facebook's name policy silenced a blogger in Honduras", *The Next Web*, 25 de octubre de 2011. http://thenextweb.com/facebook/2011/10/25/how-facebooks-name-policy-silenced-a-blogger-in-honduras/ (consultado el 16 de octubre de 2015).

Kayyali, Nadia. "Global Coalition to Facebook: 'Authentic Names' Are Authentically Dangerous for Your Users". *Electronic Frontier Foundation*, 5 de octubre de 2015. https://www.eff.org/document/open-letter-facebook-about-its-real-names-policy (consultado el 13 de octubre de 2015).

Lessig, Lawrence. *Code and Other Laws of Cyberspace.* Nueva York: Basic Books, 1999.

McKinnon, Rebecca. *Consent of the Networked: The Worldwide Struggle For internet Freedom.* Nueva York: Basic Books, 2013.

Mill, John Stuart. "Sobre la libertad" (1859). *Ateísmo Positi-*

vo, http://www.ateismopositivo.com.ar/Stuart%20Mill%20John%20-%20Sobre%20la%20libertad.pdf (consultado el 13 de octubre de 2015).

Monroy-Hernández, Andrés. "Hiding in Plain Sight: A Tale of Trust and Mistrust inside a Community of Citizen Reporters", en *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media,* Eni Mustafaraj *et al*., 2012. https://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/view/4677/4990 (consultado el 13 de octubre de 2015).

Mueffelmann, Kurt. "Uber's Privacy Woes Should Serve tAs a Cautionary Tale for All Companies", *Wired*, enero de 2015 http://www.wired.com/insights/2015/01/uber-privacy-woes-cautionary-tale/ (consultado el 16 de octubre de 2015).

Porter, Tom. "Angela Merkel challenges Mark Zuckerberg on Facebook hate speech", *International Business Times*. 26 de septiembre de 2015, http://www.ibtimes.co.uk/angela-merkel-challenges-mark-zuckerberg-facebook-hate-speech-1521412 (consultado el 15 de octubre de 2015).

Rusbridger, Alan. "The Snowden Leaks and the Public", The New York Times Review of Books, 21 de noviembre de 2013. http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/ (consultado el 16 de octubre de 2015).

Stallman, Richard. "Reasons not to use Uber", https://stallman.org/uber.html (consultado el 16 de octubre de 2015).

La violencia de género en México y las tecnologías de la información

Estefanía Vela y Erika Smith

Cuando hablamos de tecnologías de la información, libertad de expresión y género, son muchas las perspectivas e intersecciones que pueden analizarse.[1] Por ejemplo, ¿quiénes tienen acceso a estas tecnologías y para qué las utilizan?[2] ¿Quiénes participan en su diseño, producción y difusión?[3] ¿Quién tiene la posibilidad de expresarse en línea, quién no y por qué? ¿Quién es realmente leído, escuchado y compartido por acceder a espacios de poder dentro del mundo virtual? Se podría también profundizar en el contenido que se

1 Véase APC. "Feminist Principles of the Internet", *Encyclopedia of Gender and Information Technology (2 Volumes)*, Eileen M. Trauth (ed.), 2006) http://www.genderit.org/node/4097/ (consultado el 12 de enero de 2016).

2 Véase, por ejemplo, Linda A. Jackson et al., "Race, Gender, and Information Technology Use: The New Digital Divide", *CyberPsychology & Behavior*, vol. 11, núm. 4 (2008); Ricardo Hausman, Laura D. Tyson, Saadia Zahidi, "Doubling Digital Opportunities. Enhacing the Inclusion of Women & Girls in the Information Society", The Broadband Commission Working Group on Broadband and Gender, (2013); ONU Mujeres, "La Declaración y la Plataforma de Acción de Beijing Cumplen 20 años", 2015, 43-45.

3 Véase, por ejemplo, Bernhardt (2014).

produce, viendo qué refleja y cómo impacta las relaciones de género existentes.

Dentro de este universo de posibilidades, este capítulo se enfoca en un fenómeno específico: la violencia de género que se reproduce a través de las tecnologías de la información, especialmente –aunque no de manera exclusiva– la que ocurre en línea y afecta de manera desproporcionada a las mujeres.

Si bien este artículo no es exhaustivo respecto del fenómeno que analiza y las soluciones que propone, esperamos que sirva como un mapa para comenzar a navegar este tema, desde una perspectiva de política pública para el contexto mexicano. Adelantándonos un poco: la violencia de género reproducida a través de las tecnologías de la información no es algo intrínseco a la tecnología, que siempre va a suceder de manera natural. De nosotros, como sociedad completa, depende que persista o no, se intensifique o no, que encuentre nuevas avenidas para manifestarse o no, y que recaiga sobre ciertas personas, por ciertas razones.

Ahora bien, para hacer frente a esta violencia, no cualquier intervención es válida. Apelar a los derechos humanos no basta para legitimar cualquier política pública. Precisamente porque el uso de la tecnología y el flujo de la información están de por medio, se debe tener sumo cuidado al combatir la violencia. Esperamos que con este artículo quede más claro por qué las autoridades y la sociedad civil deben hacer frente a esta violencia, pero también cómo deben hacerlo sin vulnerar derechos humanos en el camino.

1. El fenómeno: la violencia de género

El foco de este artículo son los actos de violencia basada en género que son cometidos, promovidos o agravados, en parte o de manera total, por el uso de la información y la tecnología.[4] Estos actos pueden provocar un daño físico, sexual, psicológico, social y/o económico para sus víctimas, vulnerando con ello múltiples de sus derechos humanos.

El papel que juega el género en la configuración de los ataques determina a sus víctimas (desproporcionadamente mujeres), a los agresores (desproporcionadamente hombres) y a los actos que se despliegan, cuyo resultado es (re)instaurar

4 Nuestra definición de violencia de género está basada en la que utiliza la Asociación para el Progreso de las Comunicaciones (APC). Véase, por ejemplo, APC, "Tecnology-related Violence Against Women–A briefing Paper", junio de 2015, https://www.apc.org/en/system/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015.pdf (consultado el 12 de enero de 2016) pero, como podrá verse, bien puede derivarse al menos de los siguientes documentos internacionales: Comité de la CEDAW, "Recomendación General No. 19", 11º período de sesiones, 1992, http://www.un.org/womenwatch/daw/cedaw/recommendations/recomm-sp.htm#recom19 (consultado el 12 de enero de 2016); Asamblea General de las Naciones Unidas, "Declaración sobre la eliminación de la violencia contra la mujer, resolución 48/104", 20 de diciembre de 1993, http://www.ohchr.org/SP/ProfessionalInterest/Pages/ViolenceAgainstWomen.aspx (consultado el 12 de enero de 2016); *Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y violencia doméstica*, Estambul, 2011, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680462543 (consultado el 12 de enero de 2016).

un sistema de género en el que a hombres y a mujeres se les asignan ciertos roles, comportamientos, actividades, espacios y atributos que son considerados "apropiados" para su sexo.[5] Esto es, el género ayuda a entender la lógica que subyace a la violencia ¿Y cuál pretende ser uno de sus resultados?, que la "diferencia" de género quede resguardada.

Como veremos a continuación, un análisis de los casos de violencia revela cómo lo que opera en estos nuevos contextos tecnológicos son viejos estereotipos de género. Por ejemplo, que las mujeres no pueden opinar sobre ciertos temas –como la política o los deportes–, porque va más allá de lo que saben como mujeres (y si se atreven a desafiar esta expectativa, serán atacadas) o que son ellas quienes provocan la furia o el deseo de los hombres, por su comportamiento (publicando fotos "provocativas", "dejándose" tomar fotos provocativas, "siendo" provocativas), por lo que lo único que queda es que dejen de comportarse así. El re-

5 Por "sistema de género" entendemos el conjunto de ideas, normas, instituciones y prácticas que diferencian entre hombres y mujeres, asignándoles a cada "grupo" un papel, lugar y función distinta en una sociedad dada, exigiéndoles o asumiendo que despliegan (o ambos a la vez) comportamientos, intereses, actitudes y deseos distintos. El sistema que produce la diferencia de *género*: la "masculinidad" en los cuerpos concebidos como cuerpos de "hombres" y la "feminidad" en los cuerpos concebidos como de mujeres. Para esta "definición" seguimos a autoras como Joan Scott (1990), Teresa de Lauretis (1987); así como los trabajamos contenidos en Lamas (comp., 2000). Para la diferencia entre sexo y género, véase Anne Fausto-Sterling (1985/1992 y 2012) y Rebecca Jordan-Young (2011).

sultado será que las mujeres opinen exclusivamente sobre "lo que les corresponde" y que se conduzcan en estos foros como las "buenas mujeres" deben hacerlo: recatadamente, cuidando siempre no incitar a los hombres. En otras palabras, reproduciendo y perpetuando el sistema de género establecido, un sistema en el que las personas se queden en los espacios y roles que les correspondan, por el solo hecho de ser "hombres" y "mujeres".

Ahora, como veremos a continuación, esta forma de violencia no necesariamente se distingue de otras que pueden no estar basadas en el género: las amenazas son amenazas; las violaciones a la privacidad son violaciones a la privacidad; el acoso y el acecho son acoso y acecho. Pero si se quiere entender qué motiva y posibilita esta violencia en particular, el género es un lente imprescindible para ello.

Valga revisar qué clase de actos pueden ser entendidos como violencia de género reproducida utilizando las tecnologías de la información.

1.1. Difundir, sin el consentimiento de la víctima, sus datos e imágenes personales

El primer tipo de casos conectados con la violencia de género tiene que ver con la difusión, sin el consentimiento de la víctima, de imágenes o videos en los que aparece desnuda (o semidesnuda) o realizando algún acto sexual. Los ejemplos cada vez son más y algunos han sido ampliamente reportados por los medios de comunicación bajo el dudoso nombre de "pornografía de venganza". Los casos varían en

algunos detalles: las víctimas van desde actrices[6] hasta políticas,[7] pasando por mujeres sin un perfil público. Los agresores han sido desde exparejas hasta personas desconocidas (aunque predominan los agresores que conocen personalmente a las víctimas). Las filtraciones se han dado a través de celulares y dispositivos de Bluetooth,[8] páginas de Facebook, Twitter o

6 Está el caso de Ruby, una modelo y actriz de las Filipinas. Sostuvo una relación corta con un hombre –conocido como Dr. Yu–, con el que se reunía en hoteles. Un año después de haberlo conocido, un reportero le advirtió que se iba a liberar un video en el que aparecían teniendo sexo en el hotel. Se terminaron por difundir tres distintos videos en línea, mismos que fueron descargados y se comenzaron a vender como DVD. Como resultado de la difusión, Ruby fue objeto de un escarnio incesante en redes y llegó a perder múltiples oportunidades laborales. Con el tiempo, se difundieron más videos de Dr. Yu con otras mujeres. GenderIt.org, "A case study from the Philippines: An illicit video and one woman's battle for justice", http://www.genderit.org/sites/default/upload/case_studies_phil2_0.pdf (consultado el 12 de enero de 2016).

7 Está el caso de Martha, también de las Filipinas. Ella inició su carrera en el mundo del entretenimiento, pero se pasó al de la política, resultando electa como consejera municipal. Se liberaron dos fotografías suyas en Instagram, en las que aparecía semidesnuda. Sus hijos fueron "tagueados" en las imágenes. Ella también sufrió un escarnio público como resultado de esta difusión. GenderIt.org, "A case study from the Philippines: When Nude Photographs are Dragged Into the Limelight", http://www.genderit.org/sites/default/upload/case_studies_phil1_0.pdf (consultado el 12 de enero de 2016).

8 Está el caso de Aisha, una niña de Pakistán. Cuando tenía 14 años, inició una relación con un joven de 18. Dos amigos de él los grabaron teniendo sexo. Usaron el video para violarla, amenazándola con difundirlo si no se sometía. Después, fueron con el padre de ella, extorsionándolo para

Yahoo! o en sitios autodenominados pornográficos.[9] A veces no solo se liberan imágenes, sino que van acompañadas de datos personales de las víctimas (como su nombre, sus correos, sus direcciones o sus números telefónicos); en otras ocasiones, los agresores han fingido ser las víctimas, utilizando las imágenes para establecer contacto con otros hombres, haciéndoles creer que buscan una relación sexual

---

que les diera dinero a cambio del video. Al no cumplir con la exigencia, comenzaron a difundirlo utilizando la tecnología de Bluetooth a los celulares de otras personas. El padre de ella la sacó de la escuela, argumentando que era esta libertad la que la llevó a la deshonra. GenderIt.org, "A case study from Pakistan: When a sex video is used as blackmail", http://www.genderit.org/sites/default/upload/case_studies_pak3_0.pdf (consultado el 12 de enero de 2016).

9 Está, por ejemplo, el caso de Holli Thometz, una mujer de Estados Unidos. Un mes después de terminar una larga relación con su novio, Ryan Seay, apareció en su propio perfil de Facebook una foto en la que estaba desnuda. Con el paso de los meses, comenzaron a aparecer más fotos y un video de ella –junto con su nombre y correo electrónico– los que se viralizaron y llegaron a estar en más de 100.000 sitios de internet. Como resultado de esto, se vio forzada a cambiar su nombre, dejar su trabajo (era una estudiante de doctorado y asistente docente) y esconderse. El caso es relatado en Samantha Kopf (2014).

(poniéndolas en riesgo).[10] [11] En algunos de estos casos, las imágenes fueron tomadas con el consentimiento de la víctima; en otros no. En todos, sin embargo, fueron difundidas sin su consentimiento.

Esta violación a la privacidad de la víctima es parte del problema, mas no todo. Las imágenes se difunden precisamente por la concepción que se tiene de la sexualidad de una mujer en ciertas sociedades; por cómo será juzgada por los actos sexuales que aparece realizando en ellas. Se difunden porque

10 Está el caso de Cecilia Barnes, también de Estados Unidos. Su exnovio creó distintos perfiles en Yahoo! utilizando su nombre, en los que incluía imágenes de ella en las que aparecía desnuda, junto con su información laboral (su dirección, correo electrónico y teléfono). Además de incluir estos datos, el exnovio se hacía pasar por ella en salas de chat, estableciendo contacto con diferentes hombres, haciéndoles creer que ella deseaba tener sexo violento. Ella se dio cuenta de esto cuando distintos hombres la empezaron a buscar en su trabajo, algunos, incluso, apareciéndose en persona. El caso es revisado por Bartow (2013).

11 Además del caso de Thometz (supra), está el de M.B. y su exnovio, Sean Sayer, revisado también por Ann Bartow (2013). Después que ella terminó la relación con él, Sayer comenzó a acecharla "en persona", acto por el que fue condenado. Después de esto, cambió su estrategia y comenzó a utilizar las redes. Un día, apareció un hombre en su casa, alegando que se habían conocido en línea y que había accedido a tener un encuentro sexual con él. Con el paso de los días, aparecieron más hombres en su casa. Descubrió que había un perfil de ella en el sitio de Craigslist, que incluía fotografías suyas, su dirección y una lista de actos sexuales que estaba interesada en hacer. Terminó por mudarse de ciudad. Una vez ahí, volvieron a aparecer hombres en su casa. Se volvió a cambiar de ciudad por segunda vez y ocurrió lo mismo.

imágenes así sirven para, efectivamente, afectar la vida social, familiar y laboral de una mujer, porque son muestra de lo "puta" que es, algo que, en muchas sociedades, una "buena mujer" nunca debe ser.[12] Ese es el componente de género más evidente en estos casos y es la razón por la cual las imágenes que se difunden casi siempre son sexuales.[13]

El segundo componente de género constante es que quienes difunden estas imágenes muchas veces son hombres que conocen a la víctima: hombres con los que tuvieron o tienen una relación sexual o afectiva. Un patrón preocupante es que las imágenes se difunden una vez que las mujeres cortan lazos con estos hombres, siguiendo los patrones típicos de la violencia doméstica, donde esta última se intensifica precisamente cuando se quiere terminar la relación. De ahí que muchas personas insistan en llamar a este fenómeno "pornografía de venganza":[14] porque las imágenes se difunden precisamente para "vengar" al hombre agraviado que ha sido "abandonado" por una mujer (de nuevo el componente de género: una "buena mujer" no deja a su hombre).

Por la violación a la privacidad que representa la difusión de estas imágenes y por el papel que juegan en la reproduc-

12 Véase Martha Rivas Zivy (2005), Marta Lamas (2007), Sylvia Chant y Nikki Craske (2007, capítulo 6).

13 Valga la pregunta retórica: ¿serían efectivas para castigar a una mujer fotos privadas en las que aparezca sonriendo en un parque con sus hijos?

14 Según APC: "La expresión 'pornografía de venganza' es equívoca, porque lo que describe es un acto de violencia que no debe mezclarse con el contenido pornográfico" (Namita Malhorta, 2015).

ción de la desigualdad de género –castigando social, laboral y familiarmente a las mujeres por sus vidas sexuales– es el primer fenómeno al que se le debe hacer frente, si se busca combatir la violencia de género reproducida con las tecnologías de la información.

1.2. Amenazar a la víctima utilizando a las tecnologías de la información

Un segundo tipo de casos conectado con la violencia de género son las amenazas. A veces, éstas pueden ir acompañadas de un acecho físico constante a la víctima, como se ha visto en casos que involucran exparejas[15], y otras pueden ser recurrentes y estar relacionadas con el trabajo que realizan las víctimas. Existen también casos en que se amenaza a la víctima con difundir información personal de manera ilegal –como lo puede ser un video o una fotografía de naturaleza sexual– si no se somete a los "deseos" del agresor. La tecnología se utiliza para extorsionar a la vieja usanza, en clave de género.

15 Está, por ejemplo, el caso de Rebecca de Bosnia y Herzegovina. Cuando decidió terminar la relación con su expareja, precisamente porque era violento, él se dedicó a acecharla. La seguía al trabajo, se paraba afuera de su casa, se aparecía en los cafés o clubes nocturnos que ella visitaba. Comenzó a mandarle mensajes amenazantes a su celular, algo que se intensificó cuando ella empezó a salir con otro hombre; por más de un mes les enviaba a ambos mensajes de esta naturaleza a sus celulares. Cuando ella acudió a la policía, no tomaron ningún tipo de acción, hasta que la expareja cumplió sus amenazas y la golpeó. GenderIt.Org, "A Case Study from Bosnia and Herzegovina: When an ex-boyfriend's violence turns digital", http://www.genderit.org/sites/default/upload/case_studies_byh3_0.pdf (consultado el 12 de enero de 2016).

Por ejemplo, el caso de una pareja de lesbianas que vivían en el Estado de México y que se dedicaban al activismo a favor de los derechos de las lesbianas. Además de recibir por años llamadas a sus celulares en las que les solicitaban servicios sexuales, llegaron a recibir amenazas por correo electrónico, en sus celulares y en sus blogs. Las amenazas eran de distintos tipos: que iban a quemar su casa, que sabían dónde estaban y a qué hora se reunían y que iban a violar a su hija.[16]

También está el caso de una madre lesbiana que defendió el derecho de su hijo a no ser discriminado por llevar el pelo largo en una escuela privada del estado de Sonora. Cuando el caso se mediatizó, la madre empezó a recibir amenazas por Twitter, en las que le decían que la iban a violar, a golpear o a matar por "pervertir" a su hijo "convirtiéndolo" en "una niña". Algunos de los mensajes iban acompañados por fotografías de metralletas; en una de ellas, aparecía una nota con el nombre de la madre al lado del arma.[17] Ella no

16 GenderIt.Org, "A Case Study from Mexico: Persistent Harassment Plagues Lesbian Activists", http://www.genderit.org/sites/default/upload/case_studies_mex2_0.pdf (consultado el 12 de enero de 2016).

17 Para entender cómo surge este caso, véase Estefanía Vela Barba, "Por escuelas libres de estereotipos", *El Universal*, 23 de septiembre de 2015, http://www.eluniversal.com.mx/blogs/estefania-vela-barba/2015/09/23/por-escuelas-libres-de-estereotipos-de-genero (consultado el 12 de enero de 2016); para entender los argumentos que se utilizaban para discriminar a la madre por su orientación sexual, véase Estefanía Vela Barba, "Por sociedades libres de estereotipos", *El Universal*, 1 de octubre de 2015, http://www.eluniversal.com.mx/blogs/estefania-vela-

fue la única que recibió este tipo de amenazas: su abogada y dos columnistas que habían defendido su actuación también fueron objeto de amenazas similares, en las que, por ejemplo, se llamaba a "violarlas" para "corregirlas" por ser "lesbianas".

Estos dos casos ilustran bien lo que nos preocupa: lo que pasa aquí son amenazas tradicionales pero se conectan con el género tanto por lo que las motiva (amedrentar a quienes cuestionan el sistema de género con su trabajo, su sexualidad o su maternidad), como por la forma que a veces toman las amenazas (se intimida a mujeres con "violarlas", no solo con golpearlas o matarlas). Las amenazas nos preocupan por el impacto que tienen en la seguridad física y emocional de las víctimas, así como por el efecto que pueden tener en la misma libertad de expresión. Si por hablar o defender derechos esto es lo que una persona recibe, ¿quién, entonces, querrá hablar?

1.3. Difamar a la víctima

El tercer tipo de casos que nos preocupa es la difusión de información diseñada para dañar la imagen de la víctima.

---

barba/2015/10/1/por-sociedades-libres-de-estereotipos (consultado el 12 de enero de 2016); para las amenazas de las que fueron objeto la madre, su abogada y las columnistas (incluyendo a la autora de este texto), véase Catalina Ruiz Navarro, "Trolls y acceso a derechos", 28 de septiembre de 2015, disponible en: http://catalinapordios.com/2015/09/28/trolls-y-acceso-a-los-derechos/ (consultado el 12 de enero de 2016).

Valgan dos ejemplos. El primero es el de una mujer[18] acusada de serle infiel a su marido en una página comunitaria, cuestionando si sus hijos eran realmente de él. Este dato falso corrió entre su comunidad, llegando a su marido, de quien eventualmente se divorció.[19] Es un ejemplo típico –clásico, incluso– de difamación social, con la novedad que se reproduce a través de las nuevas tecnologías de la información. También tenemos el caso de la activista por los derechos de las mujeres conocida como Menstruadora, que es un ejemplo paradigmático de difamación política.[20]

18 GenderIt.Org, "A Case Study from Mexico: a Defamatory Facebook Profile Brings Violence into Marriage", disponible en: http://www.genderit.org/sites/default/upload/case_studies_mex4_0.pdf (consultado el 12 de enero de 2016).

19 Está el caso de Séraphine, del Congo. Su exnovio, al enterarse que ella estaba saliendo con otro hombre, comenzó a publicar imágenes de ella en línea, con comentarios ofensivos ("Aquí está la puta preparándose para otra noche en la que le es infiel a su marido"); subía imágenes de él mismo haciéndose exámenes de infecciones de transmisión sexual alegando que de seguro "le había pegado algo"; borraba cualquier comentario a favor de Séraphine (pero no los múltiples proferidos por otras personas que la insultaban), incluidas sus propias explicaciones de lo que estaba ocurriendo. Entró de manera ilegal al blog de ella y ahí también incluía este tipo de información; consiguió la lista de correos de familiares y amigos de ella y les envió un correo explicándoles "su versión" de los hechos. GenderIt.Org, "A Case Study from Democratic Republic of Congo", http://www.genderit.org/sites/default/upload/case_studies_rdc1_1.pdf (consultado el 12 de enero de 2016).

20 Artículo 19, "Alertas: Amenazas de muerte a feminista y comunicadora, grave ataque a la libertad de expresión", 22 de mayo de 2015, http://articulo19.org/amenazas-de-muerte-a-feminista-y-comunicadora/

Además de los constantes mensajes en los que se llamaba a violarla o matarla o los intentos por conseguir su información personal (rastrear los eventos a los que iba, conseguir su dirección, etcétera), varias personas comenzaron a circular a través de Twitter y Facebook mensajes en los que la acusaban de cometer actos de "pedofilia" y que advertían que no había que dejar que las niñas "cayeran" en sus manos. Esto porque Menstruadora, junto con otras activistas, abrió un taller feminista para niñas y adolescentes, que supuestamente las ponía en peligro. Sin el más mínimo sustento, la información corría por cuanto espacio fuera posible.

De nuevo: estos casos son como muchos otros de difamación; su conexión con el género es, otra vez, lo que los motiva (desacreditar a quien con su trabajo cuestiona el sistema de género) o la manera en la que busca desacreditarse a la víctima (cuestionando su apego al mismo sistema de género).

1.4. Acechar a la víctima utilizando las tecnologías

El cuarto tipo de casos que nos preocupa tiene que ver con el constante monitoreo de la víctima, utilizando las tecnologías.[21] Aquí también pueden darse distintos supuestos. Puede

---

(consultado el 12 de enero de 2016); Catalina Ruiz Navarro, "La sangrona", *El Modernísimo*, 20 de mayo de 2015, disponible en: https://elmodernisimo.wordpress.com/2015/05/20/la-sangrona/ (consultado el 12 de enero de 2016).

21 En múltiples artículos académicos no siempre se distingue entre lo que nosotros llamamos acoso (*harassment*) y acecho (*stalking*). Creemos que esto se debe, en parte, a que los comportamientos muchas veces pueden ir de la mano: por ejemplo, ante un rechazo, una misma persona

tratarse de una persona que, a través de las redes, establece contacto con la víctima y hace todo lo posible por tener una relación con ella, incluso después que esta ha manifestado su rechazo; sus mensajes no cesan y siempre encuentra una manera de hacerse presente en la vida de la víctima. Puede utilizar la información disponible en línea para descifrar los lugares en los que se va a encontrar la víctima y aparecerse ahí; puede buscar establecer contacto con los allegados de la víctima y aprovecharlo para obtener información o tratar de presionar a la víctima a tener una relación; puede entrar de manera ilegal a las cuentas de la víctima para obtener información que sirva para manipularla. Más allá de que estos actos culminen o no con un acto ulterior de violencia (un ataque, una violación, etcétera), el acecho en sí representa una violación a la autonomía y privacidad de la víctima que, además, provoca miedo y un sentido de vulnerabilidad: si no se respetan los deseos de la víctima, ¿qué más no se va a respetar?[22]

---

puede acosar a la víctima en las redes, insultándola o amenazándola; al mismo tiempo, puede estar por completo pendiente de los lugares que visita y las personas que frecuenta, haciéndole saber en todo momento su presencia. Hemos distinguido entre ambos supuestos, sobre todo porque el acoso puede no siempre devenir en acecho; y el acecho puede no necesariamente implicar actos de acoso (si no actos que, desde la perspectiva del perpetrador, son "inofensivos" y "hasta románticos"). Véase, por ejemplo, Bradford et al (2012), Laura J. Moriarty & Kimberly Freiberger (2008), Cristina Cavezza & Troy E. McEwan (2014), L.P. Sheridan & T. Grant (2007).

22 GenderIt.Org, "A Case Study from Bosnia and Herzegovina: An Obsession Turns Violent Across Digital Platforms", http://www.genderit.org/sites/default/upload/case_studies_byh2_0.pdf (consultado el 12 de enero de 2016).

En otros casos, el monitoreo a través de las tecnologías es un acto de control y violencia que despliega el agresor en contra de la víctima, con la que está o ha estado en una relación sentimental. Entran de manera no consentida o incluso ilegal a sus cuentas personales, para controlar con quién hablan y lo que dicen, o utilizan el dispositivo GPS del celular para saber dónde están a todo momento.[23] También pueden hacerse pasar por la víctima, enajenando a sus amistades o familiares. El caso del acecho es un perfecto ejemplo de cómo el comportamiento no es un fenómeno nuevo; lo novedoso radica en las formas que las personas tienen para ejercer el control o monitorear a una persona: utilizando la tecnología digital.

1.5. Acosar a la víctima a través de la tecnología

En quinto lugar, encontramos los casos de "acoso" propiamente dicho.[24] Como han señalado varias académicas, esto

23 Esto ha llegado no solo a afectar las vidas de cada víctima en lo individual, sino incluso las medidas de seguridad que tienen que tomar los centros de atención a víctimas de violencia doméstica. Véase, Cindy Southworth & Sarah Tucker (2007), Jill P. Dimond et al (2011), Aarti Shahani (2014).

24 Existe un estudio realizado para el *Pew Research Center* dedicado al acoso en línea, que desagrega los distintos tipos de acoso que sufren las personas y queda claro que los hombres y las mujeres no son víctimas en la misma proporción de estos distintos tipos de acoso. Por ejemplo: si se analizan cuántas personas han sido "insultadas" (*called offensive names*), el número de hombres y mujeres que han vivido este tipo de acoso es casi idéntico (51% versus 50%); si nos enfocamos en las amenazas físicas, el 26% de los hombres han sido amenazados versus el 23% de las mujeres; pero si vemos el acecho, la desproporción es mucho más grande: solo el 7% de los hombres han vivido esto versus el

puede comprender una serie de distintos tipos de actos (Barak, 2005; Franks, 2012). Por ejemplo, el envío de imágenes o comentarios sexuales no deseados. Es decir, mujeres que en sus correos o cuentas personales de Facebook –por ejemplo– reciben fotografías de penes o comentarios sexuales ("eres una puta", "¿quieres coger?", "enséñame tus tetas").

También encontramos casos de mujeres que, sin recibir directamente este tipo de comentarios, se convierten en el objeto de una discusión en línea: los usuarios las califican conforme a su deseabilidad sexual; describen lo que les harían ("me la chingo", "yo sí la violo", etcétera); discuten la vida sexual (real o no) de la víctima, por lo general, empleando términos sexistas (como "puta", "perra", etcétera).[25] Un ejemplo emblemático es el de una estudiante de la Universidad de Vanderbilt, quien se enteró que se había abierto un foro en el sitio Juicycampus.com en el que se hablaba de la violación que había sufrido, afirmando, además, que "se lo merecía" (Franks, 2012,680). El problema, encima de lo que

---

26% de las mujeres; lo mismo ocurre con el acoso sexual: el 13% de los hombres han sufrido acoso sexual, versus el 25% de las mujeres. Este es un claro componente de género en cómo se vive el acoso en línea (Duggan, 2014).

25 Uno de los casos más famosos en Estados Unidos es el del sitio Autoadmit.com, un foro en el que las personas podían compartir información sobre las escuelas de derecho (cuáles son las mejores, cómo son los procesos de admisión, cuáles son los despachos más importantes, etcétera). Las mujeres que se convirtieron en "objeto" de discusión eran estudiantes de facultades de derecho, por lo general (Franks, 2012, 678).

le provoca a la víctima, es que luego estos "mensajes" aparecen en búsquedas de internet, como las que pueden realizar, por ejemplo, empleadores o clientes (potenciales o actuales), afectando las opciones laborales de las víctimas.

Por último, están los mensajes "sexistas" que pueden recibir mujeres al participar en un foro ("¡Vete a tu lugar natural que es la cocina!", "Cállate, puta", "Eres la mujer más fea que he visto", etcétera)[26] que, como ha señalado la académica Mary Anne Franks, en contextos como el laboral y el escolar no serían tolerados (Franks, 2012,680). El acoso en línea es, quizá, el fenómeno que puede llegar a involucrar al mayor número de personas. Una sola víctima puede recibir cientos de miles de mensajes al día de esta naturaleza, cada uno de distintas personas. Dependiendo del caso, este problema se puede agravar si se libera información privada de la víctima, incluida su dirección personal o de trabajo (fenómeno conocido como *doxxing*), poniéndola en peligro.

1.6. Otras formas de violencia

Además de los cinco tipos de casos que hemos identificado, pueden existir otros. Los últimos ejemplos que nos preocupan son los de censura propiamente dichos: cuando cuentas de redes sociales o sitios web de mujeres o de grupos activistas feministas son atacadas para "bajarlas" o "suspenderlas", afec-

26 En Amanda Hess (2014) se incluyen ejemplos bastante "ilustrativos" de la clase de comentarios que reciben mujeres como ella que se dedican a escribir en línea.

tando su libertad de expresión.[27] Como todos los casos que hemos revisado, este ejemplo también se relaciona con el género, ya sea en lo que motiva el ataque o cómo se manifiesta.

Ahora, si bien hemos agrupado los casos en diferentes tipos, nada impide que, en los hechos, todos los actos de violencia se desplieguen a la vez. Una expareja puede acceder ilegalmente a las cuentas de la víctima, obteniendo de esta manera información privada; puede difundir imágenes sexuales de la víctima sin su consentimiento; puede monitorearla, amenazarla y ponerla en peligro utilizando la tecnología. Todo esto puede provenir de una sola persona. Al revés, una víctima puede sufrir muchos de estos actos provenientes de varias personas (como fue el caso de Menstruadora). Los hemos separado porque, como veremos más adelante, las respuestas que cada tipo requiere pueden –y deben– ser distintas.

Vale la pena hacer algunas puntualizaciones: 1) no es necesario que la víctima tenga una presencia en línea o que ella misma utilice la tecnología para que sea víctima de este tipo de violencia. Puede darse el caso de una mujer que es grabada sin su consentimiento y cuyo video es difundido en línea sin que se entere, sino hasta años después. 2) Si bien hace falta más información, es importante notar que en varios de los casos que hemos estudiado las víctimas pueden agruparse en dos tipos: o se trata de figuras públicas y politizadas (como defensoras de derechos humanos, feministas, activistas) o se trata de mujeres que estuvieron o están en una relación de

27 Como ejemplo, véase Jasper Hamill (2015).

violencia. Este es el componente de género más sobresaliente, de hecho: las víctimas son mujeres que se salen de los roles estereotípicamente asignados (la mujer callada, dócil, que acepta a su hombre de manera incondicional). Aquí precisamente es donde también caben las víctimas que son violentadas por su orientación sexual o identidad de género, o por el trabajo relacionado con ello que llevan a cabo; que desafían con sus vidas o expresiones al sistema de género.

Que se reconozca el componente de género no quiere decir que las mujeres sean las únicas a las que amenazan o monitorean en línea, o las únicas susceptibles a invasión de su privacidad, extorsión, difamación o insultos de manera incesante. Tampoco significa que cualquier ataque a una mujer sea un ataque basado en el género. Toda la violencia debe ser atendida; el punto es entender cómo funciona en cada caso particular. De ahí que la lente del género sea importante en términos de políticas públicas.

2. Violencia de género y derechos humanos vulnerados

La violencia de género puede provocar un daño físico, sexual, psicológico, social y económico para sus víctimas. Este segundo apartado tiene como propósito ahondar en cuáles son los derechos humanos que vulnera la violencia de género que se inflige utilizando las tecnologías de la información, conforme al marco jurídico mexicano actual.

Como se verá, no es necesario reconocer nuevos derechos para intervenir en este fenómeno, pues estos ya se encuentran contemplados. Lo que hace falta, más bien, es legis-

lación secundaria adecuada –eficiente, eficaz y apegada al mismo régimen de derechos humanos– para hacerle frente a la violencia.[28] Repasaremos los derechos humanos básicos que sirven para dar sustento a cualquier política pública que quiera realizarse sobre la materia, como lo son el derecho a la vida privada, el derecho al respeto a la honra o reputación, el derecho a la integridad física, psíquica y moral, el derecho a la no discriminación por género y el derecho a la libertad de expresión.

2.1. El derecho a la no discriminación por razón de género

El primer derecho que nos parece clave para hacer frente a la violencia que hemos identificado es, precisamente, el de la no discriminación por razón de género. Este es un derecho que protege a las personas frente a un trato diferenciado, cuando este tiene como motivo o se relaciona con su género. La doctrina de este derecho es enfática en señalar que la discriminación ocurre no solo a través de actos intencionales,

28 Como queda claro del análisis de los casos que presentamos en el apartado anterior, la gran mayoría de los actos de violencia que identificamos fueron realizados por "particulares" en contra de "particulares". Desde nuestra perspectiva, esto no impide hablar de una violación a los derechos humanos de la víctima. Al reconocer la Constitución que el Estado está obligado a proteger los derechos humanos, está reconociendo que estos se pueden ver vulnerados por terceros –y no solo por el mismo Estado–. De ahí que nos permitimos hablar de una vulneración a los derechos de la víctima, incluso cuando esta proviene de un particular, considerando que esto es lo que le genera al Estado la obligación de hacer algo al respecto (de proteger). Para la explicación de cada una de las obligaciones estatales, seguimos el trabajo doctrinal expuesto en Víctor Abramovich y Christian Courtis (2002).

sino cuando existen prácticas que terminan por impactar a las personas de manera diferenciada de acuerdo al género.

El derecho a la no discriminación y al trato igualitario también sirve para proteger a las personas de discriminaciones motivadas por otras causas, como lo son la raza, la clase o la orientación sexual. Muchos de los casos que nos preocupan tienen un trasfondo de género: el control o castigo a personas por salirse de los mandatos propios del género. Mujeres que osan dejar a sus maridos; chicas que rechazan los avances de un hombre; mujeres que ejercen libremente su sexualidad; feministas que critican el sistema patriarcal; estudiantes o trabajadoras que acceden a espacios tradicionalmente masculinos. Seguir permitiendo actos como los que hemos identificado perpetúa que las mujeres se queden en los roles y espacios a los que tradicionalmente han sido asignadas: castas, calladas, sometidas a un hombre y fuera de "lo público" como puede ser un trabajo o el mismo ciberespacio. Podríamos afirmar que el derecho a la no discriminación por género es el primer derecho clave para justificar cualquier intervención en esta materia y que atraviesa los múltiples casos que hemos identificado.

2.2. El derecho a la libertad de expresión

El segundo derecho clave que nos parece justifica la necesidad de actuar frente a la violencia de género que se inflige utilizando las tecnologías de la información es el de la misma libertad de expresión, en un sentido amplio. Uno de los impactos que tiene la violencia, especialmente el acoso y las amenazas constantes, es que las víctimas empiezan a

moderar lo que expresan, moderando también su uso de la tecnología y las redes de comunicación.

Son varias los mecanismos de autocensura y cautela que se pueden tomar, como guardar silencio por miedo a la violencia que reciben por sus opiniones (que no es lo mismo que dejar de emitir una opinión porque genuinamente han sido convencidas de sus "errores" argumentativos); hacer "privadas" sus cuentas de redes sociales limitando el alcance que pueden tener sus expresiones, así como los intercambios positivos que podrían obtener por ello, o dejar de participar, de plano, en el diálogo social. Con ello, el debate se encarece.[29]

Y este es precisamente el punto de proteger la libertad de expresión en una democracia. Es un derecho que tiene, como lo ha reconocido en múltiples ocasiones la Suprema Corte, dos dimensiones:[30] una individual, conectada con el derecho

29 Para el caso del acoso en línea, el argumento de que "disminuye la expresión" ha sido desarrollado extensivamente por Anita Bernstein (2014). Es un argumento que, en términos más generales, ha sido desarrollado por Owen Fiss (1998).

30 "Libertad de expresión. Dimensiones de su contenido, Pleno de la Suprema Corte de Justicia de la Nación", *Semanario Judicial de la Federación y su Gaceta*, tomo XXV, mayo de 2007, 1520, Jurisprudencia P./J. 25/2007, registro número 172479; Libertad de expresión y derecho a la información. Su importancia en una democracia constitucional, Primera Sala de la Suprema Corte de Justicia de la Nación, *Semanario Judicial de la Federación y su Gaceta*, tomo XXX, diciembre de 2009, 287, tesis 1ª. CCXV/2009, registro número 165760; Libertad de expresión. este derecho fundamental se relaciona con principios que no pueden reducirse a un solo núcleo, Primera Sala

al libre desarrollo de la personalidad; y otra social o política, conectada con la deliberación democrática. Ambas dimensiones están implicadas en el caso de la violencia de género en línea: las víctimas dejan de utilizar las redes para desarrollar su "autonomía" y expresar lo que sea que quieran expresar, por más trivial o trascendental que sea; y por otro lado, el público deja de tener acceso a una opinión o punto de vista valioso para el debate, algo no menor cuando las víctimas son activistas, columnistas, académicas o personas que se dedican a realizar análisis valiosos para la democracia, o simplemente cuando se trata de personas comunes que no merecen exclusión del debate público.

En México, el caso más emblemático de esto es, una vez más, el de Menstruadora, quien, ante las amenazas constantes que recibió cerró sus cuentas de Twitter y Facebook. Esto representa no solo una vulneración de su propia libertad de expresión, sino del derecho a la información de todos y todas: una voz crítica que se perdió.

Ahora bien, es importante reconocer que no solo está implicada la libertad de expresión de la víctima, sino de cualquier

---

de la Suprema Corte de Justicia de la Nación, *Semanario Judicial de la Federación y su Gaceta*, libro 13, diciembre de 2014, tomo I, p. 236, tesis 1ª. CDXVIII/2014, registro número 2008104; Libertad de expresión. dimensión individual de este derecho fundamental, Primera Sala de la Suprema Corte de Justicia de la Nación, *Semanario Judicial de la Federación y su Gaceta*, libro 13, diciembre de 2014, tomo I, p. 233, tesis 1ª. CDXX/2014, registro número 2008100.

persona similar a ella. Ver la facilidad e impunidad con la que se puede atacar a una persona, envía un mensaje al resto del público: "así pueden acabar ustedes también si osan expresarse así". La violencia puede tener un efecto silenciador similar al que ha sido reconocido para los casos en los que el Estado castiga expresiones (Fiss, 1996).

Reconocer las implicaciones que tiene la violencia para la libertad de expresión es sumamente importante para analizar las soluciones que se le ofrecen a la víctima. Es ilegítimo pedir que para que cese la violencia simplemente se deje de utilizar la tecnología o las redes sociales. El punto, precisamente, es idear soluciones que, más que menoscabar su libertad de expresión, la protejan.

De la misma manera en la que el derecho a la no discriminación por género atraviesa todos los casos que hemos revisado, la libertad de expresión también está siempre implicada en lo que se refiere a la regulación del uso de la tecnología. Todas las políticas públicas que se emprendan en esta materia tienen que estar orientadas a potenciar la libertad de expresión, especialmente de quienes se ha identificado quedan silenciadas o excluidas del debate por un abuso de la tecnología o de la misma libertad de expresión.

2.3. El derecho a la vida privada

Más allá de los derechos transversales que obligan a las autoridades a actuar frente a la violencia de género y la tecnología, repasemos algunos de los derechos en concreto que también están implicados en la materia.

El primero es el derecho a la vida privada, que tiene una relación estrecha con los casos en los que se difunden datos personales o imágenes de "naturaleza sexual" sin el consentimiento de la víctima.[31] También lo tiene con los casos en los que una persona accede a las cuentas personales de la víctima, sin su consentimiento, sea que difunda la información o no.

Este derecho se encuentra contenido en el artículo 11 de la Convención Americana sobre Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos que, explícitamente, establecen que nadie puede ser objeto de injerencias arbitrarias, abusivas o ilegales en su vida privada.[32]

31 Sabemos que el derecho a la protección de los datos personales está explícitamente contemplado en el artículo 16, párrafo segundo, de la Constitución mexicana. Hemos decidido, de cualquier manera, enfocarnos en el derecho a la vida privada, porque tiene un carácter más amplio (y que tutela, sin lugar a dudas, la información de carácter "sexual").

32 Hemos elegido hablar de "derecho a la vida privada" siguiendo a la Convención Americana sobre Derechos Humanos y al Pacto Internacional de Derechos Civiles y Políticos. No hemos utilizado el "derecho a la intimidad", aunque reconocemos que la misma Suprema Corte de Justicia de la Nación también lo utiliza, a veces como sinónimo del derecho a la vida privada, como en el Amparo Directo Civil 6/2008 ("El derecho a la intimidad, es decir, a no ser conocidos por otros en ciertos aspectos de nuestra vida y que, por tanto, cada sujeto puede decidir revelar, es el reconocimiento del ámbito propio y reservado del individuo ante los demás, sean poderes públicos o particulares, que le garantiza el poder de decisión sobre la publicidad o información de datos relativos a su persona o familia, sus pensamientos o sentimientos. Es la plena disponibilidad sobre su vida y la decisión de lo que puede

Para la Corte Interamericana de Derechos Humanos, la vida privada abarca la capacidad de la persona "para desarrollar la propia personalidad y aspiraciones [y] determinar su propia identidad [...] Incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás" y también protege "la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos".[33]

La Suprema Corte de Justicia de la Nación (SCJN) complementa esta visión de la siguiente forma:

> [L]a protección constitucional de la vida privada implica poder conducir parte de la vida de uno protegido de la mirada y las injerencias de los demás, y guarda conexiones de variado tipo con pretensiones más concretas […]: el derecho de poder tomar libremente ciertas decisiones relativas al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de la integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho

---

revelar de su intimidad a los demás", p. 87), otras veces como lo que parece ser una subespecie del mismo, como en el Amparo Directo en Revisión 2044/2008 ("[La Corte] también ha subrayado la relación de la vida privada con [...] el derecho a la intimidad, y ha sugerido la posibilidad de entender el derecho a la vida privada como un concepto más general, abarcativo de los tres –honor, privacidad e intimidad–, aunque hay desde luego motivos para que tenga pleno sentido hacer, en sede constitucional, distinciones nítidas entre ellos", p. 24).

33 Corte Interamericana de Derechos Humanos, *Atala Riffo y niñas vs. Chile*, párr. 162.

> a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, […] la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular.[34]

Como queda claro de las palabras de la SCJN, las imágenes de "naturaleza sexual" y los datos personales quedan cubiertos por la protección del derecho a la vida privada. Las personas tienen el derecho a que este tipo de información privada no sea difundida sin su consentimiento. Esto es sumamente importante, sobre todo considerando que hay quienes creen que la solución al problema de la difusión de imágenes sexuales no consentida es que las mujeres dejen de tomarse fotografías. Adoptar una política pública de este tipo no solo no resolvería el problema, sino que vulneraría el derecho a la vida privada, ya que requeriría que las personas dejen de cometer ciertos actos constitucionalmente protegidos –como tomarse fotografías eróticas–, porque algunas personas ilegalmente abusan de ellas. Cualquier política pública que se emprenda tiene no solo que respetar este derecho (no exigiéndoles a las personas que renuncien a actos constitucionalmente protegidos), sino protegiéndolo de quienes abusan de él.

Ahora, por supuesto que este derecho puede verse limitado; la misma Suprema Corte concede que puede haber un con-

34 Amparo Directo en Revisión 2044/2008, 23-25.

flicto entre la libertad de expresión que se ejerce al difundir esta información y el derecho a la vida privada de la persona cuyos datos y/o imágenes son difundidas.

Un primer requisito para determinar si se violó o no el derecho a la vida privada tiene que ver con el carácter de la información que se difundió: si es de interés público o no. En ninguno de los casos anteriormente expuestos podríamos decir de manera inequívoca que la información es de interés público. Esta se define como "la información que el público considera relevante para la vida comunitaria",[35] lo cual haría posible argumentar que ni siquiera cuando la información es de actrices o políticas ("figuras públicas"), se justifica difundir imágenes de naturaleza sexual, salvo que se demuestre que sean absolutamente necesarias para discutir un asunto de interés público (como podría ser evaluar el trabajo de un político o una política).[36]

35 Amparo Directo 3/2011, 87. "Otra forma de expresar esta idea es que la información íntima sólo puede considerarse de interés de la colectividad cuando su difusión contribuya al debate público o lo enriquezca. En este sentido, existirá un legítimo interés "de conocer lo que incide sobre el funcionamiento del Estado, o afecta intereses o derechos generales, o le acarrea consecuencias importantes' a la sociedad." *Ibíd.*, 90-91.

36 Por ejemplo: puede darse el supuesto que se difundan imágenes en las que aparece un político con una mujer que trabaja para él. Podría llegar a argumentarse que es de interés público saber si el político está cometiendo un acto de abuso de poder (como lo es el acoso sexual laboral). Otro ejemplo: puede darse el supuesto de un político que reiteradamente emprende acciones en detrimento de las trabajadoras sexuales, que se presenta como un "hombre de familia" y resulta

En los casos en que las imágenes fueron tomadas con el consentimiento de las víctimas, tampoco se justifica la invasión a su vida privada, ya que tenían una expectativa de confidencialidad cuando accedieron a ello. Para la Corte, "una comunicación es *confidencial* cuando se lleva a cabo en circunstancias en las que se puede asumir razonablemente que las partes indican su deseo de mantener confinada dicha información",[37] que es exactamente lo que ocurre cuando se acepta este tipo de interacción al interior de una relación. La expectativa es de confidencialidad, no de publicidad. De ahí su vulneración.

2.4. El derecho al respeto de la honra o reputación

El derecho al respeto de la honra o reputación sirve, entre otras cosas, para proteger a las personas de la difusión de información falsa, diseñada para afectar la reputación de la que gozan frente a terceros. Este derecho se encuentra contenido en el artículo 11 de la Convención Americana sobre Derechos

---

que le es infiel a su esposa con trabajadoras sexuales. Este tipo de información puede considerarse de interés público, ya que evidencian una contradicción entre su carácter y actos y la ideología que dice sostener. El problema con los casos que hemos identificado es que ni siquiera existe ese vínculo entre lo que las imágenes "muestran" y el trabajo de una mujer. Las imágenes solo muestran que es "sexual"; no que está traicionando alguna ideología política o cometiendo un delito. No son de interés público; no permiten hacer una crítica válida en un sistema constitucional comprometido con la igualdad de género; esto es, con un mundo en el que las mujeres son valoradas por su trabajo y no exclusivamente por la vida sexual que llevan

37 *Ibíd.*, 98.

Humanos y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, mismos que establecen que "nadie puede ser objeto de ataques ilegales a su honra o reputación".

El caso más evidente de este supuesto es el de la activista Menstruadora, quien fue acusada de cometer actos de pedofilia, en múltiples ocasiones, a través de las redes sociales (como Twitter y Facebook, entre otras). También son relevantes los casos en los que las imágenes de las personas son adulteradas para aparecer, por ejemplo, en pornografía.

Por supuesto que la protección del derecho a la honra o a la reputación debe también considerar la libertad de expresión. La Suprema Corte ha establecido múltiples principios que sirven para diseñar un marco legislativo y para emitir fallos que sean respetuosos de ambos derechos. Por ejemplo, se tiene que tomar en consideración si la expresión en cuestión se trata de una crítica sobre un asunto de interés público; se tiene que analizar quién es la persona criticada (si es o no una figura pública); se tiene que estudiar la debida diligencia de quien emitió la expresión; entre otros.[38]

38 Estas ideas han sido reiteradas por la Suprema Corte en varios casos ya, por lo que nos atrevemos a afirmar que forman su "doctrina" ya consolidada de la libertad de expresión. Véase el Amparo Directo en Revisión 2044/2008, Amparo Directo 6/2009, Amparo Directo 28/2010 y Amparo Directo 3/2011 de la Primera Sala de la Suprema Corte de Justicia de la Nación.

2.5. El derecho a la integridad física, psíquica y moral, y el derecho a la protección de la salud

El artículo 5 de la Convención Americana sobre Derechos Humanos protege el derecho de toda persona a que "se respete su integridad física, psíquica y moral". El artículo 4 de la Constitución mexicana y el artículo 12 del Pacto Internacional de Derechos Económicos, Sociales y Culturales, por su parte, protegen el derecho de toda persona "al disfrute del más alto estándar posible de salud física y mental". Estos derechos nos parecen clave para combatir múltiples actos de violencia de género, como lo son los de acecho y las amenazas. Una sola amenaza puede ser suficiente para mermar el bienestar de una persona, se cumpla o no. El acecho es también una merma constante no solo a la autonomía de la persona, sino a su seguridad y tranquilidad mental. Precisamente por eso deben ser combatidos.

2.6. Otros derechos

La violencia de género también pone en riesgo otros derechos. Está el derecho más amplio a tener "una vida libre de violencia", reconocido en la Convención de Belém do Pará (artículo 3), siempre implicado en estos casos. Asimismo, a través del acecho y el monitoreo constante de la víctima, puede violentarse su derecho a la libertad ambulatoria o a "circular libremente", reconocido en el artículo 12 del Pacto Internacional de Derechos Civiles y Políticos. Con la difusión sin el consentimiento de la víctima de imágenes sexuales puede vulnerarse su derecho a la libertad en términos de autonomía sexual, sometiéndola a un castigo social por simplemente ejercer su sexualidad.

Puede llegar a vulnerarse el derecho de la víctima a no ser discriminada en su trabajo, ya no en razón de género, sino más bien si como resultado de las imágenes que se difunden, pierde oportunidades laborales. También se puede afectar a la víctima en su derecho a la protección de su vida familiar, si como resultado de la violencia estas son afectadas, por ejemplo, si se cuestiona la calidad "maternal" de la víctima y se pone en riesgo la relación que tenga con sus hijos o hijas. Sin duda, se tendrán que considerar estos derechos también a la hora de hacer frente a la violencia, siempre poniendo atención a los múltiples efectos que puede tener en la vida de una persona.

3. Soluciones y propuestas de política pública

En este apartado vamos a revisar el tipo de soluciones que se requieren para prevenir, detener y castigar esta violencia, soluciones, sin embargo, que tienen que apegarse al mismo marco de los derechos humanos. Partimos de la premisa que no cualquier intervención en esta materia es válida, por más que se haga en nombre de los derechos humanos. Como mínimo, las soluciones tienen que ser respetuosas de la misma libertad de expresión y del debido proceso.

3.1. Ejes de acción

Queremos comenzar este apartado apuntando a los múltiples ejes de acción que deben considerarse si se quiere hacer frente a esta violencia. Posteriormente nos vamos a enfocar en quiénes y cómo tienen que implementar estas soluciones; pero por ahora queremos señalar de manera general que los esfuerzos tienen que enfocarse en al menos lo siguiente:

- Detener la violencia. Una de las consecuencias más preocupantes de la difusión de imágenes sexuales sin el consentimiento de la víctima no solo es la posibilidad de que se "viralice" (esto es, que siga difundiéndose), sino que quede perpetuamente accesible al público. Que cada vez que se hace una búsqueda del nombre de la víctima en línea –como la pueden hacer futuros empleadores– aparezca. Parte de los esfuerzos tienen que estar encaminados a hacer frente a este fenómeno, porque de lo contrario se estaría revictimizando a la persona constantemente. Otro ejemplo particularmente relevante para los casos de acoso: que existan mecanismos que dificulten o impidan que el agresor siga contactando a la víctima. Más allá de que se castigue o no, tiene que existir la posibilidad que la violencia se detenga.

- Proteger a la víctima. Los esfuerzos también tienen que enfocarse en proteger a la víctima, algo particularmente relevante para los casos de amenazas o de acecho. Esto tiene que contemplar desde el resguardo y protección de sus datos y aparatos (esto es, ofrecerle soluciones tecnológicas para la protección de sus datos), hasta su seguridad física.

- Sancionar al agresor. Parte de los esfuerzos también deben ir encaminados a sancionar al perpetrador de la violencia, esto es, asegurar la consecuencia del reproche normativo por afectación de bienes jurídicos.

- Prevenir la violencia. Por último, los esfuerzos tam-

bién deben ir encaminados a prevenir la violencia. ¿A qué nos referimos con esto? Primero: entender que este tipo de violencia está conectada con una desigualdad de género que permea todos los ámbitos de la vida. Si no existe un combate generalizado en contra de la desigualdad, la violencia de género reproducida a través de la tecnología seguirá reapareciendo una y otra vez. El ejemplo más obvio es en relación a la violencia y desigualdad doméstica: si no se abordan las causas que la provocan, en general, de poco servirán los esfuerzos que se hagan para combatir la que ocurre a través de la tecnología.

Segundo: la prevención de la violencia también pasa por la denuncia constante del fenómeno en múltiples escenarios, como lo pueden ser la escuela o las mismas redes. Tienen que existir espacios para que las personas aprendan sobre ella, entendiendo las consecuencias que tiene en las vidas de las personas.

Tercero: tiene que haber un esfuerzo para que las personas conozcan sus derechos, así como las herramientas que tienen para protegerse de la violencia (por ejemplo: conocer los aparatos y las plataformas que utilizan y sus medidas de privacidad).[39]

39 Al proponer esto, sin embargo, queremos advertir sobre un punto: este tipo de estrategias tienen que evitar poner la responsabilidad en la víctima sobre la violencia de la que es objeto. El punto de estas iniciativas tiene que ser empoderar a las personas, que sepan cuáles son las herramientas que ellas mismas pueden utilizar para fortalecerse; no responsabilizarlas de la violencia de la que son objeto.

3.2. ¿De dónde deben venir las soluciones?

Como segundo punto, creemos importante señalar que para hacer frente a la violencia, el Estado no es el único que puede estar implicado en los esfuerzos, ni es el derecho la única herramienta que puede servir para ello.

Todo actor que forme parte del proceso de comunicación y del desarrollo tecnológico debe involucrarse. Queremos destacar el papel fundamental que podrían desempeñar los mismos intermediarios,[40] y en especial los proveedores de contenido en internet. Es decir, las plataformas que manejan la distribución de contenido en línea y la hacen accesible a los usuarios.[41] Ejemplos de esto son, por un lado, administradores de nombres de dominio y servicios de alojamiento de contenido, como Godaddy o Dreamhost; y por otro, las redes sociales como Facebook y Twitter, que alojan contenido ajeno.[42]

Una categoría distinta son los motores de búsqueda de internet como Google o Yahoo!, que si bien no alojan ni crean conteni-

40 OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, OECD Publishing, 2011.

41 J. Jay Darrington, "What is an Internet Content Provider?", *Small Business* , 28 de enero de 2015, http://smallbusiness.chron.com/internet-content-provider-57363.html (consultado el 2 de febrero de 2016).

42 Gisela Pérez de Acha, Censura de Desnudos Femeninos en Facebook: Violación a la libertad de expresión por empresas privadas en internet, Tesis de licenciatura en Derecho, ITAM, 2015, 22; Rebecca MacKinnon *et al., Fostering Freedom Online. The Role of Internet Intermediaries*, UNESCO, 2014, 22, http://unesdoc.unesco.org/images/0023/002311/231162e.pdf (consultado el 2 de febrero de 2016).

do, hacen una agregación de información que luego es desplegada en orden como resultados de búsqueda de palabras.

Más allá de las obligaciones legales de estas compañías, puede existir un esfuerzo para que adopten como propio el combate en contra de la violencia de género. Como ejemplo, en junio de 2015, Google creó un mecanismo para que las personas puedan solicitar que imágenes sexuales difundidas sin su consentimiento sean removidas de los buscadores, si bien no de la web entera.[43] Por otro lado, en diciembre de 2015, Twitter amplió la categoría de "abuso" para permitir que las amenazas violentas, el acoso y las conductas de odio pudieran ser correctamente denunciadas.[44]

En la misma línea, Riot Games, creadores de uno de los videojuegos más populares en línea, *League of Legends*, desarrollaron un sistema para identificar, castigar y prevenir el abuso en el juego[45] que está mostrando una efectividad alen-

43 Amit Singhal, "'Revenge porn' and Search", Google Public Policy, 19 de junio de 2015, http://googlepublicpolicy.blogspot.mx/2015/06/revenge-porn-and-search.html (consultado el 12 de enero de 2016).

44 The Twitter Rules. *Twitter Help Center*. 28 de enero de 2015, https://support.twitter.com/articles/18311# (consultado el 12 de enero de 2016).

45 Simon Parkin, "A Video-Game Algorithm to Solve Online Abuse", *MIT Technology Review*, 14 de septiembre de 2015, http://www.technologyreview.com/news/541151/a-video-game-algorithm-to-solve-online-abuse; Laura Hudson, "Curbing Online Abuse Isn't Impossible. Here's Where We Start", *Wired*, 15 de mayo de 2014, http://www.wired.com/2014/05/fighting-online-harassment (consultado el 12 de enero de 2016).

tadora, demostrando cómo en el mismo diseño de las plataformas se puede fomentar o desincentivar la violencia.

También queremos destacar la importancia del desarrollo de herramientas tecnológicas para combatir la violencia. La campaña Take Back the Tech, por ejemplo, se ha dedicado a proveer a las personas herramientas para la protección de sus datos y aparatos. La organización Hollaback ha desarrollado una plataforma llamada HeartMob para detectar, documentar y combatir el acoso en línea.[46] La misma tecnología es una apuesta más para combatir la violencia.[47]

3.3. Soluciones provenientes del Estado

Para concluir, haceremos un repaso de las intervenciones mínimas que se pueden adoptar desde el mismo Estado para comenzar a hacer frente a la violencia de género perpetrada a través de las tecnologías de la información. La lista que presentamos definitivamente no es exhaustiva; sirve simplemente para proveer una guía de acciones mínimas.

46 Sarah Kessler, "Meet HeartMob: A Tool for Fighting Online Harassment Designed by People who have been Harassed", *Fast Company*, http://www.fastcompany.com/3046181/tech-forecast/meet-heartmob-a-tool-for-fighting-online-harassment-designed-by-people-who-hav (consultado el 12 de enero de 2016).

47 Ceri Hayes, *Tackling Gender-Based Violence with Technology*, STATT, 2014, http://www.genderit.org/sites/default/upload/statt_tackling_gbv_with_technology.pdf (consultado el 12 de enero de 2016).

3.3.1. Identificar la conducta como comportamiento a sancionar

Uno de los primeros puntos que se debe revisar es si las conductas que hemos identificado como problemáticas deben o no ser reconocidas como ilícitos a sancionar por el Estado. El segundo punto es determinar a través de qué mecanismo deben ser sancionadas: si mediante derecho penal, derecho civil u otras vías.

Desde nuestra perspectiva, no toda la violencia que hemos identificado amerita ser catalogada como una falta jurídica. En concreto, pensamos en el acoso en el sentido de maltrato. Si bien este puede ser sumamente problemático para las víctimas, consideramos que la utilización de una sanción estatal de cualquier tipo para hacerle frente es excesivo y peligroso para la misma libertad de expresión. No consideramos que le corresponda al Estado monitorear y sancionar cada uno de los mensajes discriminatorios que se profieren en línea y que sumados constituyen acoso. Las soluciones en relación al acoso deberían provenir de la misma sociedad civil, de una cultura de la denuncia social, de plataformas comprometidas con diseñar soluciones óptimas para las víctimas y espacios seguros y libres de discriminación.

El resto de la violencia que hemos identificado, como la difusión de imágenes privadas y datos personales sin el consentimiento de la víctima, las amenazas, los mensajes difamantes y el acecho, por el contrario, sí nos parece que debe ser catalogada como un ilícito. ¿Qué clase de ilícito? Depende. Consideramos que el derecho penal debe utilizarse solo de

manera extraordinaria. Desde esta perspectiva, por ejemplo, los mensajes difamatorios no tienen por qué pertenecer al ámbito del derecho penal; pueden ser abordados perfectamente bajo el paradigma de reparación del derecho civil y su protección de la imagen de las personas. Reiteramos que, en todo momento, la regulación de los actos de violencia que hemos identificado debe estar apegada al marco de la libertad de expresión: las faltas deben estar claramente delimitadas en ley y ser necesarias, proporcionales y razonables para proteger derechos.[48]

En este punto, valga hacer varias aclaraciones: la violencia que hemos identificado puede ya estar cubierta por la legislación actual. No siempre será necesario realizar una reforma legislativa para hacer frente a esta violencia. Para el caso del Distrito Federal –ahora Ciudad de México–, por ejemplo, existe la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen, que sirve para cubrir tanto los mensajes difamatorios, como la difusión sin el consentimiento de la víctima de imágenes privadas o datos personales. No consideramos que sea necesario identificar estas faltas como algo distinto a lo ya existente; si bien tienen una conexión con la desigualdad de género, no siempre es necesario que se explicite en su articulación legal. Una violación de la privacidad es una violación de la privacidad.

48 Seguimos tanto la doctrina de la SCJN, como la que ha establecido la Corte Interamericana de Derechos Humanos. Véase Sergio García Ramírez y Alejandra Gonza (2007).

También puede darse el supuesto que un mismo acto ya esté contemplado en dos legislaciones distintas. Por ejemplo, si la difusión sin el consentimiento de la víctima es realizada por un excónyuge, no solo constituye una violación a la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen, sino al mismo Código Penal del Distrito Federal y su tipificación de la violencia familiar, que actualmente cubre la violencia psicológica y la sexual. El caso del acecho, cuando proviene de una pareja o expareja, también queda cubierto en el delito de violencia familiar.

3.3.2. Establecer mecanismos de protección para las víctimas

Más allá que se legislen como faltas ciertas conductas que ameriten un castigo impuesto por el Estado, consideramos fundamental establecer mecanismos para proteger a las víctimas; mecanismos que no necesariamente estén conectados con un proceso civil o penal. Muchas veces las víctimas solo quieren que la violencia se detenga y no necesariamente están dispuestas a invertir tiempo y recursos en demandar penal o civilmente a alguien. El Estado tiene, por lo tanto, que contemplar esta posibilidad a través, por ejemplo, del establecimiento de órdenes de protección, que son medidas emitidas por las autoridades para ordenar ciertos actos que protegen a las víctimas de la violencia, por ejemplo ordenándole a un agresor que deje de contactar a la víctima.

En México, este es un mecanismo al que no se le ha dado la debida atención. Son pocas las legislaciones que los contemplan; y las que incluyen estos mecanismos, los han diseña-

do de manera abstracta (como es el caso de la Ley General de Víctimas) o acotada. Como ejemplo, está la misma Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, que contempla las órdenes de protección "de emergencia, preventivas y de naturaleza civil".[49] Si se analizan, sin embargo, sirven de poco para hacer frente a la violencia que hemos identificado en este texto. Por ejemplo: las órdenes de protección de emergencia funcionan para prohibirle al probable responsable acercarse al domicilio, lugar de trabajo o estudio, o cualquier otro que frecuente la víctima; también sirven para prohibirle intimidar o molestar a la víctima en su entorno social. Valga la pregunta: ¿Abarca esto el contacto en línea? ¿El envío de mensajes o llamadas telefónicas?

Ahora, el problema de estas órdenes es que solo pueden durar un máximo de 72 horas; y se emiten por la autoridad competente una vez que ha conocido hechos que pueden constituir una infracción o delito. No existe un mecanismo que le prohíba al agresor contactar a la víctima por un periodo más amplio, algo que nos parece necesario contemplar; y no queda siempre claro si existe la posibilidad de obtener estas medidas sin hacer una denuncia penal o civil de los actos, algo que tendría que considerarse. Por supuesto, además de revisar el diseño de legislativo de las órdenes de protección, es necesario revisar que no existan barreras en el acceso efectivo a este mecanismo, como pueden ser las que surgen con el tratamiento de la víctima por parte de las autoridades.

49 Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, artículos 27-34.

Dada la naturaleza de la violencia que nos preocupa aquí, consideramos importante también establecer mecanismos que sirvan para la protección de los datos y aparatos de la víctima. Tienen que existir espacios o instituciones en las que se le pueda brindar asesoría tecnológica para salvaguardar su información y proteger sus aparatos.

3.3.3. Establecer mecanismos para restringir contenido ilícito en línea

Consideramos necesario establecer mecanismos para restringir el acceso a contenido en línea, como una de las medidas básicas para hacer frente a la difusión de imágenes privadas o datos personales de la víctima sin su consentimiento. Estos mecanismos son distintos a los que se deben diseñar para sancionar la conducta. Más que estar dirigidos a los agresores, estos mecanismos estarían diseñados para obtener la cooperación de los intermediarios de internet, en los que se reproducen o alojan las imágenes. En el diseño de estos mecanismos, tiene que existir un apego a estándares de libertad de expresión y debido proceso, tales como los Principios de Manila sobre la Responsabilidad de los Intermediarios.[50] De acuerdo a estos, nunca se puede responsabilizar a los intermediarios por el contenido producido por otras personas; lo que sí se puede hacer es solicitarles que restrinjan el acceso al contenido, con una

50 "Principios de Manila sobre Responsabilidad de los Intermediarios. Guía de Buenas Prácticas que delimitan la responsabilidad de los intermediarios de contenidos en la promoción de la libertad de expresión e innovación", marzo de 2015, https://www.manilaprinciples.org/es (consultado el 12 de enero de 2016).

orden judicial en la que se justifique cuidadosamente la solicitud, argumentando porqué el contenido viola las leyes.

Por supuesto, dado el funcionamiento descentralizado del internet, sabemos que es ingenuo pensar que este mecanismo sería fácil de implementar. Lo que creemos necesario es comenzar a discutir qué se requeriría para poder acceder a este mecanismo y cómo se puede hacer más efectivo.

3.3.4. Diseñar un procedimiento rápido, idóneo y apegado al debido proceso

Un punto que requiere de la más cuidadosa atención es el del diseño del proceso, tanto para el castigo de ciertas conductas, como para la emisión de las órdenes de protección. Es aquí donde se vuelve necesario entender la arquitectura del internet y el funcionamiento de la tecnología.

Queremos resaltar tres puntos que ameritan atención. El primero es la importancia que se diseñen procedimientos verdaderamente expeditos, especialmente para la emisión de órdenes de protección y de solicitudes de restricción de contenido. El propósito es que la acción tanto protectora como sancionadora del derecho refleje la velocidad con que la afectación de los derechos se produce en el uso de tecnologías de información y comunicación.

El segundo punto tiene que ver con cómo se prueban los hechos ante una autoridad judicial. Supongamos un caso en el que una mujer recibe amenazas a través de Twitter, Facebook y su correo electrónico. ¿Qué tiene que hacer con esa información para que se admita como evidencia en un tri-

bunal? ¿Basta tomar un pantallazo, imprimirlo y someterlo como prueba? ¿Es necesario que la recopilación de la información se realice con un notario público que de fe de los hechos? Si para cuando se admite la demanda, el contenido ya ha sido borrado y lo único que quedan son las capturas de la víctima, ¿qué ocurre? Evidentemente, las autoridades tendrán que adquirir la tecnología necesaria para recabar y recuperar datos de distintos aparatos. Y se tienen que establecer reglas probatorias claras, adecuadas y eficientes para este tipo de casos.

Un tercer punto que queremos señalar es el de la identificación del agresor. La víctima no siempre tendrá claro quién es la persona responsable del ataque. Si bien en materia penal esto no es necesario para iniciar un proceso –corresponde a la autoridad determinar el probable responsable–, un proceso civil usualmente exige identificación. Tienen que establecerse mecanismos que posibiliten la identificación del sujeto responsable. Esto, evidentemente, implica que las autoridades tienen que disponer de personas capacitadas para tal efecto.

Cualquiera que sea el esfuerzo que se realice, sin embargo, se debe contemplar el impacto que puede tener en la misma libertad de expresión, en general, y en el derecho al anonimato, en particular.[51] No se debe olvidar que solo en casos

51 Véase el Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye, Consejo de Derechos Humanos, Naciones Unidas, 22 de mayo de 2015, A/HRC/29/32, disponible en: http://daccess-dds-ny.un.org/doc/UNDOC

extraordinarios, a través de un proceso en el que se respeten diversas garantías, se puede exigir *–ex post facto–* que una compañía entregue la información privada de un usuario de internet, como su dirección IP. Los criterios de proporcionalidad y razonabilidad siempre deben guiar las acciones que se emprendan al regular todo lo relativo al uso de las tecnologías de la información, por el impacto desmedido que puede tener en la libertad de expresión.

3.3.5. Capacitación de las autoridades para el manejo de esta violencia

No queremos dejar de mencionar la importancia que tiene la capacitación de las autoridades y funcionarios públicos (jueces, fiscales, miembros de las policías) para que las leyes se puedan aplicar efectivamente. Esta capacitación tiene que hacerse al menos respecto de dos puntos:

- La tecnología en sí misma. Las autoridades tienen que tener un entendimiento de cómo funciona la tecnología y el internet. Se han documentado casos en los que las autoridades ni siquiera entienden qué son plataformas como Twitter, por lo que no dimensionan el impacto que pueden tener en la vida de una persona; o casos en los que las autoridades creen que porque ocurre en línea, no tiene impacto en la vida "real" de la víctima.[52] Esto se tiene

---

/GEN/G15/095/88/PDF/G1509588.pdf?OpenElement (consultado el 12 de enero de 2016).

52 Véase Hess (2014) y véanse los distintos casos documentados por GenderIt.Org en "Cases on Women's Experiences of Technology-Related VAW and their Access to Justice", http://www.genderit.org/

que remediar. El grado de conocimiento y especialización que tengan las autoridades dependerá, obviamente, de la función específica que desempeñan. Quienes están encargadas de investigar delitos, por ejemplo, no solo deben entender la tecnología, sino saber manejarla.

- La desigualdad de género, específicamente los estereotipos de género. Ya existen en México una multiplicidad de esfuerzos encaminados a capacitar a las autoridades en materia de género; estos esfuerzos deben conectarse al tema del uso de la tecnología. Se deben identificar las barreras más comunes que existen para que las víctimas obtengan justicia en esta materia. Por ejemplo: que la reacción de las autoridades ante la difusión de imágenes sexuales sin el consentimiento de la víctima no sea que "se lo buscó".

3.3.6. Otras acciones

Como último punto, nos gustaría repasar otro tipo de acciones que se deben emprender si se quiere combatir la violencia de género que hemos revisado:

- Sistemas de información e investigación del fenómeno. Un gran problema es la falta de información que existe sobre el problema. Esto se tiene que remediar. Se tiene que buscar la forma de comenzar a documentar el fenómeno para poder hacerle frente.

---

resources/cases-women-s-experiences-technology-related-vaw-and-their-access-justice (consultado el 12 de enero de 2016).

- Campañas de derechos digitales. Debe existir un esfuerzo para difundir los derechos digitales que tienen las personas, así como información sobre las herramientas –jurídicas y tecnológicas– que tienen para protegerse. Tiene que cuidarse, de cualquier forma, que las campañas no responsabilicen a las víctimas de su propia violación o que propongan dejar de utilizar las redes o la tecnología como solución. Por ejemplo, se deben evitar las campañas que, ante la difusión ilegal de imágenes sexuales, propongan que las personas se dejen de tomar este tipo de imágenes. Este tipo de imágenes es parte de su misma libertad de expresión y libre desarrollo de la personalidad –es legítimo que se tomen las fotos–. Lo que no lo es, es que se difundan sin su consentimiento. Las campañas podrían estar dirigidas, más bien, a alertar a las personas a que es un ilícito difundir imágenes sin el consentimiento de la víctima; a enseñarle a las personas dónde pueden denunciar este ilícito y qué clase de medidas pueden emprender para detener la difusión de las imágenes.

- Insistir en la no discriminación por género de las personas. Uno de los problemas de la difusión de imágenes sexuales sin el consentimiento de la víctima o de la difamación es, precisamente, el daño a la imagen de la víctima; que por ello, por ejemplo, se quede sin trabajo. Consideramos fundamental insistir en la importancia del derecho a la no discriminación por género en todos los ámbitos –incluido el laboral–, para no permitir que se revictimice a las personas.

- Cuidar el uso del derecho penal, específicamente en lo que se refiere a la pornografía infantil. Nos parece preocupante utilizar tipos penales actuales –como el de la pornografía infantil– para abordar fenómenos como el de la difusión de imágenes sin el consentimiento de la víctima. Se han documentado casos en otros países en los que se ha criminalizado no solo a quienes difunden la imagen sin el consentimiento de la víctima, sino a la misma víctima, cuando es menor de edad.[53] Se tiene que vigilar que no se criminalice a la víctima; y que los tipos penales se usen para lo que fueron diseñados.

4. Conclusiones

El tema de la violencia de género reproducida a través de las tecnologías de la información es relevante para al menos dos agendas: la de la igualdad de género y la de la libertad de expresión.

Desde la perspectiva de la igualdad de género, la violencia

53 Emily Clark, "Six Plymouth Students Charged in Sexting Incident", *The Patriot Ledger*, 9 de julio de 2015, http://www.patriotledger.com/article/20150709/NEWS/307109997 (consultado el 12 de enero de 2016); Kassondra Cloos & Julie Turkewitz, "Hundreds of Nude Photos Jolt Colorado School", *New York Times*, 6 de noviembre de 2015; http://www.nytimes.com/2015/11/07/us/colorado-students-caught-trading-nude-photos-by-the-hundreds.html (consultado el 12 de enero de 2016); Sarah Thompson, "Sexting Prosecutions: Minors as a Protected Class from Child Pornography Charges", *University of Michigan Journal of Law Reform*, 27 de octubre de 2014, http://mjlr.org/2014/10/27/sexting-prosecutions-minors-as-a-protected-class-from-child-pornography-charges/ (consultado el 12 de enero de 2016).

es un fenómeno viejo, que se está manifestando a través de nuevos medios y espacios. La violencia es la misma; cómo se perpetúa es lo que ha cambiado. A la lucha por erradicarla de las calles, las casas, las escuelas y el trabajo, se suman los esfuerzos por combatir la que ocurre en el ciberespacio y a través de las tecnologías de la información. Violencia que, como todas, tiene consecuencias en las vidas de las personas.

Una de las consecuencias importantes es la afectación a la misma libertad de expresión: el resultado de la violencia de género, después de todo, es hacer del ciberespacio un lugar inhóspito para las personas –específicamente, de nuevo, para las mujeres–. De ahí que se trate de un tema relevante para la misma agenda de la libertad de expresión y de los derechos digitales. La violencia de género no solo implica el abuso de la libertad de expresión de quien la perpetra –quedando desprotegida de la tutela de este derecho–, sino que afecta la libertad de expresión de quien la recibe, incluso de quien no es su objeto directo, y de la sociedad completa. No se trata, por lo tanto, de un tema que contraponga los intereses de quienes luchan en contra de la violencia y quienes buscan proteger los derechos digitales. Todo lo contrario: es un punto de convergencia.

La lucha en contra de este tipo de violencia de género debe involucrar no solo al Estado, sino a la misma sociedad civil. Y, si se quiere combatir adecuadamente, no basta enfocarse solamente en el castigo de ciertas conductas, sino en su prevención y en la protección de las víctimas. En fomentar espacios libres de violencia y de discriminación, incluso utili-

zando la tecnología misma. Al mismo tiempo, precisamente porque está vinculada con la discriminación en general, no se puede desconectar las acciones que se hacen en relación a la tecnología, con las que se hacen en el resto de los ámbitos de las vidas de las personas como lo son el trabajo, las escuelas, las calles y las familias.

Lo que se tiene que cuidar en todo momento, sin embargo, es que no se castigue a la tecnología por los abusos que de ella deriven. En el combate a la violencia no todo se vale; en el nombre de los derechos humanos de las víctimas, no se pueden cometer atropellos injustificados a la misma libertad de expresión y al debido proceso; ni se puede privilegiar siempre a los aparatos más coercitivos del Estado –como lo es el derecho penal– para hacerle frente. El mismo marco de los derechos humanos antes expuesto es el que debe guiar la lucha en contra de la violencia de género.

Abramovich, Víctor y Christian Courtis. *Los derechos sociales como derechos exigibles.* España: Trotta, 2002.

Artículo 19. "Alertas: Amenazas de muerte a feminista y comunicadora, grave ataque a la libertad de expresión". 22 de mayo de 2015. http://articulo19.org/amenazas-de-muerte-a-feminista-y-comunicadora/ (consultado el 12 de enero de 2016)

Asamblea General de las Naciones Unidas. "Declaración sobre la eliminación de la violencia contra la mujer, Resolución 48/104". Nueva York: onu, 20 de diciembre de 1993. http://www.ohchr.org/SP/ProfessionalInterest/Pages/ViolenceAgainstWomen.aspx (consultado el 12 de enero de 2016)

Association for Progressive Communications. "Tecnology-related Violence Against Women–A briefing Paper". *APC*, junio de 2015. https://www.apc.org/en/system/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015.pdf (consultado el 12 de enero de 2016)

Barak, Azy. "Sexual Harassment on the Internet". *Social Science Computer Review*, vol. 23, núm. 1, 77-92. 2005.

Bartow, Ann. "Bad Samaritanism: Barnes v. Yahoo! And Section 230 ISP immunity". En *Cyberspace Law: Censor-*

ship and regulation of the Internet, editado por Hannibal Travis. Londres y Nueva York: Routledge, 2013.

Bernhardt, Sonja. "Women in IT in the New Social Era: A Critical Evidence-Based Review of Gender Inequality and the Potential for Change". Pennsylvania: IGI Global, 2014.

Bernstein, Anita. "Abuse and Harassment Diminish Speech". *Pace Law Review*, vol. 35, 1-29. New York: Pace University School of Law, 2004.

Cavezza, Cristina y Troy E. McEwan. "Cyberstalking versus off-line stalking in a forensic sample". *Psychology, Crime & Law*, vol. 20, núm. 10, 955-970. New York: Routledge, 2014.

Chant, Sylvia y Nikki Craske. *Género en Latinoamérica*. México: CIESAS, 2007.

Clark, Emily. "Six Plymouth Students Charged in Sexting Incident", *The Patriot Ledger,* 9 de julio de 2015. http://www.patriotledger.com/article/20150709/NEWS/307109997 (consultado el 12 de enero de 2016).

Cloos, Kassondra y Julie Turkewitz. "Hundreds of Nude Photos Jolt Colorado School", *The New York Times*, 6 de noviembre de 2015. http://www.nytimes.com/2015/11/07/us/colorado-students-caught-trading-nude-photos-by-the-hundreds.html (consultado el 12 de enero de 2016).

Comité para la Eliminación de la Discriminación contra la Mujer. *Recomendaciones generales.* Nueva York: ONU

Mujer. http://www.un.org/womenwatch/daw/cedaw/recommendations/recomm-sp.htm#recom19 (consultado el 12 de enero de 2016).

Darrington, Jay. "What is an Internet Content Provider?", *The Houston Chronicle*, 28 de enero de 2015. http://smallbusiness.chron.com/internet-content-provider-57363.html (consultado el 12 de enero de 2016).

Dimond, Jill P., Casey Fiesler y Amy S. Bruckman. "Domestic violence and information communication technologies". *Interacting with Computers*, vol. 23, núm. 5, 413-421. Oxford: Oxford University Press, 2011.

Duggan, Maeve. "Online Harassment", *Pew Research Center*, 22 de octubre de 2014. http://www.pewinternet.org/2014/10/22/online-harassment (consultado el 12 de enero de 2016).

Fausto-Sterling, Anne. *Myths of Gender. Biological Theories about Women and Men*. Nueva York: Basic Books. 1ª edición 1985, 2ª edición 1992.

Fausto-Sterling, Anne. *Sex/Gender. Biology in a Social World*. Nueva York: Routledge, 2012.

Fiss, Owen. "El efecto silenciador de la libertad de expresión". *Isonomía,* núm. 4. México: ITAM-Fontamara, 1996.

Fiss, Owen. *The Irony of Free Speech*. Massachusetts: Harvard University Press, 1998.

Franks, Mary Anne. "Cyberlaw: Sexual Harassment 2.0". *Maryland Law Review,* vol. 71, 655-704. Maryland: University of Maryland, 2012.

García Ramírez, Sergio y Alejandra Gonza. "La libertad de expresión en la jurisprudencia de la Corte Interamericana de Derechos Humanos". México: CIDH y CDHDF, 2007. http://www.corteidh.or.cr/sitios/libros/todos/docs/libertad-expresion.pdf (consultado el 2 de febrero de 2016).

GenderIT.org. "Cases on women's experiences of technology-related VAW and their access to justice". *GenderIT*, 8 de enero de 2015. http://www.genderit.org/node/4221 (consultado el 12 de enero de 2016).

Hamill, Jasper. "Sexist hackers bring down feminist website on International Women's Day in bid to 'silence' female activists", *The Mirror*, 9 de marzo de 2015. http://www.mirror.co.uk/news/technology-science/technology/sexist-hackers-bring-down-feminist-5298072 (consultado el 12 de enero de 2016)

Hausman, Ricardo, Laura D. Tyson y Saadia Zahidi. "Doubling Digital Opportunities. Enhacing the Inclusion of Women & Girls in the Information Society". *The Broadband Commission Working Group on Broadband and Gender*. UNDP, 2013.

Hayes, Ceri. "Tackling Gender-Based Violence with Technology". STATT, 2014. http://www.genderit.org/sites/

default/upload/statt_tackling_gbv_with_technology.pdf (consultado el 2 de febrero de 2016)

Hess, Amanda. "Why Women Aren't Welcome on the Internet", *Pacific Standard*, 6 de enero 2014. http://www.psmag.com/health-and-behavior/women-arent-welcome-internet-72170 (consultado el 12 de enero de 2016)

Hudson, Laura. "Curbing Online Abuse Isn't Impossible. Here's Where We Start", *Wired*, 15 de mayo de 2014. http://www.wired.com/2014/05/fighting-online-harassment/ (consultado el 12 de enero de 2016)

Jackson, Linda, Yong Zhao, Anthony Kolenic III, Hiram E. Fitzgerald, Rena Harold y Alexander Von Eye. "Race, Gender, and Information Technology Use: The New Digital Divide", *CyberPsychology & Behavior*, vol. 11, núm. 4. Michigan: Michigan State University, 2008.

Jordan-Young, Rebecca. *Brain Storm: The Flaws in the Science of Sex Differences.* Massachusetts: Harvard University Press, 2011.

Kaye, David. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión", 22 de mayo de 2015, A/HRC/29/32. Consejo de Derechos Humanos, Organización de las Naciones Unidas. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/095/88/PDF/G1509588.pdf?OpenElement (consultado el 12 de enero de 2016)

Kessler, Sarah. "Meet HeartMob: A Tool for Fighting Online Harassment Designed by People who have been Harassed", *Fast Company,* 14 de mayo de 2015. http://www.fastcompany.com/3046181/tech-forecast/meet-heartmob-a-tool-for-fighting-online-harassment-designed-by-people-who-hav (consultado el 12 de enero de 2016).

Kopf, Samantha. "Avenging Revenge Porn". *The Modern American,* vol. 9, núm. 2, 22-34. Washington dc: auwcl, 2014.

Lamas, Marta (comp.). *El género. La construcción cultural de la diferencia sexual.* México: pueg, 1ª edición 2000, 3era reimpresión 2003.

Lamas, Marta. "Las putas honestas, ayer y hoy". *Miradas feministas sobre las mexicanas del siglo XX,* Marta Lamas (ed.), 312-348. México: Fondo de Cultura Económica, 2007.

de Lauretis, Teresa. *Technologies of Gender.* Indiana: Indiana University Press, 1987.

MacKinnon, Rebecca, Elonnai Hickock, Allon Bar y Hae-in Lim. "Fostering Freedom Online. The Role of Internet Intermediaries". París y Nueva York: unesco e Internet Society, 2014. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf (consultado el 2 de febrero de 2016).

Malhorta, Namita. "Basta de violencia: derechos de las mujeres y seguridad en línea. Buenas preguntas sobre

violencia relacionada con la tecnología". *APC*, marzo de 2015, http://www.genderit.org/sites/default/upload/flow_namita_malhotra_20150225_es.pdf (consultado el 12 de enero de 2016).

Moriarty, Laura J. & Kimberly Freiberger, "Cyberstalking: Utilizing Newspaper Accounts to Establish Victimization Patterns". *Victims & Offenders,* vol. 3, núm. 2, 131-141. New York: Routledge, 2008.

ONU Mujeres. *La Declaración y la Plataforma de Acción de Beijing Cumplen 20 años*. Nueva York: ONU Mujeres, 2015.

Organization for Economic Co-operation and Development. *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. Washington DC: OECD Publishing, 2011.

Parkin, Simon. "A Video-Game Algorithm to Solve Online Abuse", *MIT Technology Review,* 14 de septiembre de 2015. http://www.technologyreview.com/news/541151/a-video-game-algorithm-to-solve-online-abuse/ (consultado el 12 de enero de 2016)

Pérez de Acha, Gisela. *Censura de Desnudos Femeninos en Facebook: Violación a la libertad de expresión por empresas privadas en internet*. Tesis de licenciada en Derecho. México: ITAM, 2015.

Reyns, Bradford W., Billy Henson & Bonnie S. Fisher. "Stalking in the Twilight Zone: Extent of Cyberstalking Vic-

timization and Offending Among College Students". *Deviant Behavior*, vol. 33, núm. 1, 1-25. Nueva York: Routledge, 2012.

Rivas Zivy, Martha. "Valores, creencias y significaciones de la sexualidad femenina. Una reflexión indispensable para la comprensión de las prácticas sexuales". *Sexualidades en México. Algunas aproximaciones desde la perspectiva de las ciencias sociales,* editado por Ivonne Szasz y Susana Lerner, 137-154. México: El Colegio de México, 1ª edición 1998, 1ª reimpresión 2005.

Ruiz Navarro, Catalina. "La sangrona", *El Modernísimo*, 20 de mayo de 2015. https://elmodernisimo.wordpress.com/2015/05/20/la-sangrona/ (consultado el 12 de enero de 2016)

Ruiz Navarro, Catalina. "Trolls y acceso a derechos", 28 de septiembre de 2015. http://catalinapordios.com/2015/09/28/trolls-y-acceso-a-los-derechos/ (consultado el 12 de enero de 2016)

Scott, Joan. "El género: una categoría útil para el análisis histórico". *Historia y género: las mujeres en la Europa moderna y contemporánea,* editado por James Nash y Mary Amelang. Valencia: Alfons el Magnanim, 1990.

Shahani, Aarti. "Smartphones are used to stalk, control domestic abuse victims", *NPR,* 15 de septiembre de 2014. http://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-

stalk-control-domestic-abuse-victims (consultado el 12 de enero de 2016)

Sheridan L.P. y T. Grant. "Is cyberstalking different?". *Psychology, Crime, and Law*, vol. 13, núm. 6, 627-640. New York: Rouledge, 2007

Singhal, Amit. "'Revenge porn' and Search", *Google Public Policy Blog*, 19 de junio de 2015. http://googlepublicpolicy.blogspot.mx/2015/06/revenge-porn-and-search.html (consultado el 12 de enero de 2016)

Southworth, Cindy y Sarah Tucker. "Technology, Stalking and Domestic Violence Victims". *Mississippi Law Journal*, vol. 76. Mississippi: University of Mississippi, 2007. http://www.olemiss.edu/depts/ncjrl/pdf/Southworth-Tucker%2076.3.pdf (consultado el 12 de enero de 2016)

Thompson, Sarah. "Sexting Prosecutions: Minors as a Protected Class from Child Pornography Charges". *University of Michigan Journal of Law Reform*, 27 de octubre de 2014. http://mjlr.org/2014/10/27/sexting-prosecutions-minors-as-a-protected-class-from-child-pornography-charges/ (consultado el 12 de enero de 2016)

Trauth, Eileen (ed.) "Feminist Principles of the Internet", *Encyclopedia of Gender and Information Technology*. IGI Global, 2006. http://www.genderit.org/node/4097/ (consultado el 12 de enero de 2016)

Vela Barba, Estefanía. "Por escuelas libres de estereotipos", *El Universal*, 23 de septiembre de 2015. http://www.eluniversal.com.mx/blogs/estefania-vela-barba/2015/09/23/por-escuelas-libres-de-estereotipos-de-genero (consultado el 12 de enero de 2016)

Vela Barba, Estefanía. "Por sociedades libres de estereotipos", *El Universal*, 1 de octubre de 2015. http://www.eluniversal.com.mx/blogs/estefania-vela-barba/2015/10/1/por-sociedades-libres-de-estereotipos (consultado el 12 de enero de 2016)

La criminalización de la protesta social digital

Alberto Lujambio Llamas y José David Aroesti Ventura[1]

> *"Never be afraid to raise your voice for honesty and truth and compassion against injustice and lying and greed. If people all over the world...would do this, it would change the earth."*
>
> William Faulkner

Protestar es afectar procesos políticos, sociales y culturales de una forma no rutinaria (De la Porta y Diani, 2006). Es movilizarse a favor de una causa en declaración de un propósito y como demostración pública del descontento social; ocupar un espacio en el que los cuerpos, símbolos, identidades, prácticas y discursos se encaminan a buscar o prevenir cambios dentro de las relaciones de poder institucionalizadas. (Taylor y van Dyke, 2004).

A quienes ejercen el poder no les gusta que los inconformes se hagan oír.[2] En el mejor de los casos, aquellos que detentan

1 Los autores agradecen la crucial y valiosa colaboración de Gisela Pérez de Acha en la elaboración de este artículo.

2 Véase, para una serie de ejemplos de protestas en lugares públicos: INCLO. "Take Back the Streets. Repression of Protest and Criminalization Around the World", 2013, https://www.aclu.org/files/assets/global_protest_suppression_report_inclo.pdf (consultado el 11 de enero de

el poder utilizan las armas mediáticas y de propaganda contra los disidentes; en el peor, los que protestan pagan su inconformidad con su integridad física o con su vida. Ejemplos de esto último abundan en el contexto mexicano.[3]

Para el historiador Eric Hobsbawm (2014), el verdadero sentido de la protesta es el encuentro mismo de los manifestantes y la posibilidad que tienen de acompañarse en la euforia, en el enojo y en el dolor. El resultado –tan vistoso y emotivo– de esa solidaridad tiene un efecto distinto en sus dos destinatarios: los que detentan el poder y el resto de los gobernados.

Para el poder, la protesta social es un desafío directo. La protesta exhibe la forma en la que se gobierna: a favor de un grupo de ciudadanos y nunca para todo el pueblo. Enoja a todos los tramos de gobierno porque muestra la esencia de muchas democracias institucionales: una –endulzada– lucha de clanes y no un mecanismo de asignación de derechos y obligaciones (Halabi, 2014).

Para el resto de los ciudadanos que no participan en el movi-

---

2016).

3 En muchos casos, la reacción a la protesta ha sido la desaparición forzada de aquellos que demuestran su inconformidad. Un caso ejemplar de esta forma de operar puede consultarse en la resolución del caso Radilla vs México, en el que la Corte Interamericana de Derechos Humanos falló contra el Estado mexicano por la desaparición forzada del activista Rosendo Radilla. Corte Interamericana de Derechos Humanos, Caso Radilla-Pacheco vs. Estados Unidos Mexicanos, sentencia de 23 de noviembre de 2009.

miento, pero lo observan, es una oportunidad para generar vínculos de empatía. Es una oportunidad también para reflexionar que el poder, algún día, podría enderezarse contra ellos. La protesta social logra que los profesionales empaticen con los obreros, que los heterosexuales se preocupen por los derechos de la comunidad homosexual, que la clase media vote por una opción política que se interese por combatir la pobreza, entre otros ejemplos.

Según los principios de la democracia representativa, las decisiones de un gobierno pueden ser rebatidas por la oposición legislativa o castigadas.

Con la llegada de los medios de comunicación digital y la democratización del acceso a la información, la protesta social ha encontrado un nuevo campo de acción: blogs, redes sociales, periódicos digitales, etcétera. Protestas tan diversas como las ocurridas en Brasil, Bulgaria, Egipto, México y Turquía durante el tercer lustro del siglo XXI,[4] tienen un punto claro en común: el rol central de jóvenes educados, particularmente mujeres, en la creación de una nueva forma de discusión política (Dalton, 2013). La mayoría de ellos, no mayores de treinta años, con prospectos desoladores de empleo (Muggah, 2013). La protesta social hoy utiliza internet como mecanismo de difusión, convocatoria o realización.

4 Cada país encuentra diversas razones por la que los jóvenes se levantaron. En el caso del Medio Oriente, la protesta tuvo como principal objetivo la democratización de sus respectivos países. El caso mexicano, representado por el movimiento #YoSoy132, buscaba justamente que un partido político conocido por sus prácticas antidemocráticas no llegara al poder.

Para efectos de orden en este artículo, proponemos una división de tres maneras en la que los protestantes utilizan los medios digitales para expresar su descontento o apoyo a ciertas causas:

1. Los que expresan su inconformidad utilizando los mecanismos facilitados por las redes sociales como canal de discurso. Se trata de un tipo de activismo en el que unirse a la protesta consiste en expresar mensajes y en crear tendencias destacadas para dar mayor visibilidad a la expresión o a la situación protestada. *Trending topics* en Twitter, *likes* en Facebook y firmas en plataformas como Change.org guían el debate.

2. Los que se aprovechan de la naturaleza descentralizada de internet –es decir, no controlada por un ente único de poder central– como canal de comunicación privada, para transmitir información sensible, organizarse y convocar a la protesta física. Esta información normalmente se presenta en forma de *banners*, memes, infografías, comunicados, etcétera.

3. Los que entienden a internet como una verdadera reencarnación de la plaza pública e inciden en la disponibilidad de los servicios digitales que ofrecen los gobiernos y empresas contra los cuales protestan. Este paso va más allá de la mera discusión pública, lo que significa que la protesta adquiere una verdadera dimensión digital y prescinde de cualquier espacio físico.

En este artículo se abordarán conceptualmente estos tipos

de protesta digital y cómo se aplican al contexto mexicano. Esta es una problemática sensible para nuestra democracia, ya que la manifestación del descontento en medios digitales ha sido reprimida, atacada, penada y castigada por el poder político –con un énfasis particular desde que el Partido Revolucionario Institucional (PRI) regresó a la cúspide del poder político en el año 2012.

Existen muchas preguntas que deben resolverse para poder crear un marco regulatorio que garantice este medio novedoso de protesta y que, a la vez, establezca los límites de actuación del poder público. ¿Qué aproximación se debe tomar frente a la protesta para garantizar plenamente su ejercicio? ¿Qué estándares se deben seguir y qué conductas se deben evitar? ¿Cómo maximizar el derecho a la libertad de expresión en línea y minimizar los daños de su ejercicio? ¿Cómo se aplican los principios desarrollados a lo largo de los últimos siglos a esta nueva forma de expresión ciudadana?

1. Protesta, represión y derechos

El reconocimiento de derechos individuales y colectivos puede provenir de dos procesos históricos muy concretos: la organización del poder en forma de instituciones y la organización de la disidencia en forma de protesta. Unos se inconforman con una situación fáctica o institucional con la que disienten, los otros reprimen la expresión de esas opiniones. Cuando la situación es insostenible o la represión se vuelve imposible o impráctica, se otorgan derechos.[5] En este

5 Un tercer participante en este proceso histórico son los ciudadanos

marco, los cambios sociales suelen darse a pesar de las leyes y en contra de las mismas (De la Porta y Diani, 2006).

Un punto que comparten las manifestaciones mencionadas es el uso de la plaza pública como plataforma para lanzar sus ideas y, en ocasiones, como último baluarte de su libertad. La plaza pública tiene un lugar especial en la teoría liberal democrática y ha servido como piedra fundacional en la construcción de nuestras libertades modernas (Hall, 2009). Es decir, el ejercicio de los derechos de expresión y de reunión supone la existencia de un lugar público para ese ejercicio.

A lo largo de la historia, la actividad económica, política y religiosa de cualquier ciudad se desenvolvió en la plaza pública. Mercados, edificios de gobierno y de culto público tenían un espacio predominante en la vida de los habitantes de dichas ciudades. Tan estrecho era este vínculo, que el plan maestro de cualquier ciudad colonial, como las fundadas en México por siglos, contiene un espacio central para estos tres elementos.

Sin embargo, las cosas han cambiado. Las interacciones personales, sociales y laborales las realizamos ahora también a través de medios electrónicos y digitales. No es raro, enton-

---

que no necesariamente participan en la protesta. Wayne A. Santoro (2008), argumenta que el movimiento por los derechos civiles de los afroamericanos en Estados Unidos únicamente fue posible materializarlo cuando lo que él denomina la "audiencia" o los ciudadanos no participantes en la protesta, se interesaron en el movimiento y ayudaron a ejercer presión en el gobierno.

ces, que la protesta social también se haya desplazado a dichos espacios virtuales.

¿Es posible pensar que plataformas como Facebook o Twitter son la nueva plaza pública? Después de todo, es ahí donde el flujo moderno de ideas nace y se esparce. Y, más importante aún, es en dichas plataformas donde existe la verdadera posibilidad de una audiencia.[6] Sin embargo, es importante no perder de vista su naturaleza eminentemente privada y la lógica comercial que persiguen.

El discurso público común es plantear que internet es un lugar especialmente diseñado para la manifestación de las ideas públicas, un espacio cuasi utópico en el que cualquiera tiene una voz y todos tienen una audiencia. Pero esto está muy lejos de la realidad. Internet está montando sobre una lógica de mercado y su infraestructura y control se encuentran, casi en su totalidad, en manos privadas. Servidores, cables, proveedores de servicio, intermediarios, contenido, etcétera, se encuentran protegidos bajo el manto del derecho de la propiedad privada y, en muchas ocasiones, detrás de barreras de pago. Incluso la distribución de obras del dominio público (desde material literario, obras históricas, hasta la letra de la ley) se realiza a través de medios privados. En pocas palabras, casi la totalidad del tráfico de la red de redes se encuentra en control de manos particulares.

6 Aunque los blogs personales también ofrecen algunas de las posibilidades de estas plataformas sociales, como la de expresar y difundir una idea, las denominadas "redes sociales" facilitan la existencia de una audiencia para la recepción de esa expresión.

Este es un problema que no puede obviarse en el presente análisis. Los dueños de los sitios web pueden, en cualquier momento, negar la entrada a sus servicios e información a cualquiera que quebrante sus políticas de uso (al igual que los dueños de los establecimientos físicos). Nos encontramos en un momento histórico donde los "Términos y Condiciones de Uso" se enfrentan directamente a algunos derechos fundamentales.

En este "nuevo" espacio con características tan *sui generis*, se desarrollan movimientos disidentes que conviven y retan las narrativas de un gobierno autoritario en México.

2. El disenso social digital en México

2.1. Insurrección, protesta y medios en el contexto mexicano

Una de las primeras formas en que un movimiento disidente mexicano utilizó internet, se verificó en el surgimiento del Ejército Zapatista de Liberación Nacional (EZLN): una organización indígena de Chiapas que salió a la luz pública el 1 de enero de 1994, el mismo día en que entró en vigor el Tratado de Libre Comercio de América del Norte durante el gobierno de Carlos Salinas de Gortari. Aunque su caracterización es la de una fuerza de insurrección paramilitar, sus declaraciones políticas tienen un fuerte componente de protesta contra el gobierno mexicano y el sistema político en general. En la Primera Declaración de la Selva Lacandona de 1993, establecieron como ejes: "la lucha por trabajo, tierra, techo, alimentación, salud, educación, independencia, libertad, democracia, justicia y paz (...) lograr el cumplimiento

de estas demandas básicas de nuestro pueblo formando un gobierno de nuestro país libre y democrático".[7] Si bien este movimiento parecía apuntar a intereses predominantemente regionales, pronto se convirtió en un símbolo de la lucha anti-globalización con redes de apoyo mundiales (Hernández, 2004).

Internet tenía poco tiempo de haber pasado de las manos del Departamento de Defensa de Estados Unidos, a un uso más cotidiano, privado y comercial, que partía de los correos electrónicos y se extendía a una incipiente World Wide Web. El EZLN aprovechó esas circunstancias y usó la red para sus fines, incluyendo la publicación de sus comunicados (Lane, 2003). En la primera semana después de su primer levantamiento, una enorme y compleja red internacional de apoyo e información se puso en marcha a través de este medio.[8]

Mientras los zapatistas tenían una presencia sofisticada en internet, en Chiapas existía una infraestructura muy precaria en la que algunos poblados no contaban siquiera con electricidad. Internet fue importante en este contexto, pues la visibilización internacional que dicha herramienta permitió, hizo mucho más difícil que el gobierno mexicano suprimiera información o tergiversara los hechos relacionados

7 Comandancia General del EZLN. *Declaración de la Selva Lacandona*. 1993. http://palabra.ezln.org.mx/comunicados/1994/1993.htm (Consultado el 11 de enero de 2016).

8 La página Zapatistas in Cyberspace hace un buen recuento de esta red y sus mensajes intercambiados. Revisar en http://www.indigenouspeople.net/zapatist.htm (Consultado el 11 de enero de 2016).

con su lucha (Froheling, 1997). En ese sentido, la experiencia de WikiLeaks es una manifestación más reciente de lo ya visto con el EZLN: el uso de redes digitales para saltar cercos informativos que impiden el disenso con el poder político, pero con el agregado local de la estrecha relación entre el poder político mexicano y el poder de los medios de comunicación social.[9]

Esto último no es una preocupación menor en el contexto mexicano: la omisión y el silenciamiento de toda información relativa a las demandas de los colectivos de protesta y movimientos sociales, es una práctica habitual de las principales estaciones de televisión, entre ellas Televisa y TV Az-

9 WikiLeaks es un híbrido de una solución tecnológica para publicar información sensible (de gobiernos o corporaciones) de manera anónima, y una plataforma político-mediática para incidir en la opinión pública. Funciona como depositario de documentación filtrada y a la vez como el lugar de anuncio del contenido de dichas filtraciones. WikiLeaks se convirtió en fuente importante en la opinión pública de filtraciones como el baleo en Irak de ciudadanos civiles por fuerzas norteamericanas, documentación sobre las guerras de Irak y Afganistán, y comunicaciones del personal diplomático de Estados Unidos en el mundo. WikiLeaks se convirtió así en una fuente para el descontento público, mediante el solo acto de revelación de información (Leigh, 2011). Los intentos de represión contra WikiLeaks por parte del gobierno de Estados de Unidos (perjudicado políticamente con las filtraciones), fueron múltiples y diversos. Así, se intentó cortar el financiamiento y los servidores cuando el senador Joe Liebermann calificó a la plataforma de terrorista e ilegal. WikiLeaks sobrevivió durante unos meses más cambiando de servidores y de sistema de distribución de contenido de manera diaria, con el objetivo de que los documentos filtrados pudieran seguirse diseminando, aun cuando su capacidad económica quedó mermada.

teca. Como lo señala Rovira-Sancho (2013), la historia de la televisión en México refleja la alianza del poder político con el mediático. Del año dos mil hasta hoy, han surgido movimientos sociales de extrema relevancia para la vida política del país y sistemáticamente han sido reprimidos o silenciados por este binomio de poder político y mediático. No se trata de un fenómeno novedoso: a través de los años, el poder político mexicano ha demostrado su preferencia por el uso de la fuerza en contra del descontento.[10] Su continuación en el período posterior al alza digital del EZLN cuenta con varios ejemplos de los que da cuenta Rovira-Sancho (2013).[11]

10 El antecedente más claro de esto es la matanza de Tlatelolco de 1968, en la que fueron sojuzgados miles de estudiantes a punta de gatillo y tanques de guerra, y cuando el entonces presidente Gustavo Díaz Ordaz prohibió a la prensa hablar del tema (Rodríguez, 2015).

11 Entre los ejemplos se incluyen luchas como la del Frente de Pueblos en Defensa de la Tierra en Atenco, que se opuso a la expropiación de sus tierras para la construcción de un nuevo aeropuerto en la capital del país, pero que cinco años más tarde fueron brutalmente reprimidos. En segundo lugar, la Asamblea Popular de los Pueblos de Oaxaca (APPO) que en 2006 protestó contra el entonces gobernador, Ulises Ruiz del PRI, y fueron reprimidos por los militares. En tercer lugar, el movimiento del obradorismo que surgió después de las elecciones de julio de 2006 cuando el candidato del Partido Revolucionario Democrático (PRD), Andrés Manuel López Obrador, impugnó el proceso electoral que dio la victoria a Felipe Calderón del Partido Acción Nacional (PAN). En el caso de Atenco, hubo un saldo de dos muertos, varios heridos graves, más de 200 detenidos, torturados y golpeados brutalmente, y 47 mujeres que sufrieron violación y abuso sexual por parte de agentes del Estado. Televisa y Televisión Azteca transmitieron repetidamente las imágenes de unos pobladores dando golpes de pie a un policía en

En tales casos, la reacción mediática fue siempre parecida: estos movimientos raramente aparecieron en medios masivos de comunicación y cuando lo hacían su mensaje era tergiversado: la cobertura mediática tendía a privilegiar los episodios de violencia para criminalizar a los disidentes.

Este tratamiento mediático de las protestas genera un sentimiento de indignación adicional en quienes participan del descontento. Entonces la prensa y la televisión se vuelven un motivo de protesta en sí mismo. De esta premisa parte el movimiento estudiantil #YoSoy132 que surgió durante las elecciones de 2012 usando las redes sociales como su principal plataforma, al que nos referiremos más adelante.

2.2. La protesta actual en internet

En la actualidad, México es un país con una importante población de jóvenes[12] y más de la mitad de la población tiene

---

los testículos. Cinco años después, la Suprema Corte de Justicia de la Nación determinó que los oficiales de policía hicieron un uso legítimo de la fuerza. Un recuento más detallado de los sucesos de Atenco en el año 2006 y sus posteriores consecuencias puede ser consultado en Gilly (2012).

12 Según el perfil sociodemográfico de los jóvenes, elaborado por el Instituto Nacional de Geografía y Estadística (INEGI), en México hay poco menos de 30 millones de jóvenes entre 15 y 29 años de edad. Este sector representa aproximadamente el 26,4 % de la población total. Ver Instituto Nacional de Estadística y Geografía. "Perfil sociodemográfico de jóvenes". 2010. http://www.inegi.org.mx/prod_serv/contenidos/espanol/bvinegi/productos/censos/poblacion/2010/perfil_socio/jovenes/702825056636.pdf (consultado el 11 de enero de 2016).

acceso a internet.[13] Para este grupo etario, la toma de las calles a modo de protesta se complementa con consignas elaboradas en *hashtags*; los gritos de protesta, con elaborados razonamientos expresados en blogs y periódicos digitales.

Esta generación de jóvenes hiperconectados no ha dudado en utilizar sus conocimientos técnicos para hacer valer sus derechos. Los movimientos estudiantiles de los últimos años en México han tenido una fuerte relación con plataformas sociales como Twitter y Facebook. A pesar de eso, vivimos en una era escalofriante contra el activismo digital. Como si toda la sangre derramada en la conquista y el ejercicio del derecho a protestar hubiera sido en vano (Ramlal, 2014).

Casi dos décadas después del zapatismo, los jóvenes mexicanos volvieron a utilizar internet para manifestar su descontento con las condiciones en la que se desenvolvieron las elecciones presidenciales del año 2012. Las elecciones, en su opinión, no garantizaban un campo de equidad mínimo para todos los candidatos, ya que los medios de comunicación masiva en México (radio, televisión y prensa) apoyaban desproporcionadamente y abiertamente a un solo candidato. Los medios de comunicación en el país se encuentran altamente

13 Según el estudio de "Usos y Hábitos de Internet 2015", elaborado por la Asociación Mexicana de Internet (AMIPCI), más de la mitad de la población mexicana tiene acceso a internet, lo que convierte a México en uno de los países más conectados de la región. Ver AMIPCI. "11º estudio sobre los hábitos de los usuarios de internet en México 2015". 2015. https://amipci.org.mx/images/AMIPCI_HABITOS_DEL_INTERNAUTA_MEXICANO_2015.pdf (consultado el 11 de enero de 2016).

concentrados (Mancinas, 2008) y los estudiantes buscaban su democratización.

El movimiento #YoSoy132 comenzó en la Universidad Iberoamericana de la Ciudad de México, después de la visita de campaña del ahora presidente Enrique Peña Nieto a dicha institución. Durante su estancia se le cuestionó sobre los acontecimientos de Atenco en el año 2006 (cuando aún era gobernador del Estado de México). Su respuesta desató la ira de los estudiantes, que terminaron obligándolo a salir del lugar.

La polémica por la protesta se radicalizó cuando varios actores cercanos a la campaña de Peña Nieto acusaron a los estudiantes vociferantes de "porros", "resentidos" y "peones" del candidato de la oposición, Andrés Manuel López Obrador. Días después, 131 estudiantes produjeron un ingenioso video para Youtube donde afirmaron ser estudiantes de la universidad, con credencial académica en mano, y estar en contra de la manipulación mediática que, según sus palabras, representaba la candidatura del PRI. Con la etiqueta #YoSoy132 comenzaron a popularizarse mensajes de apoyo a los 131 estudiantes: ser el estudiante 132 significaba adherirse al movimiento y apoyarlo. Fueron meses en el que las redes sociales parecían llenas de candor y esperanza.

Este movimiento se aprovechó de dos de los tipos de activismo digital previamente expuestos: facilitó una sencilla adhesión utilizando el *hashtag* #YoSoy132 y convocó a la protesta en la plaza pública por medio de las redes sociales.

También en este contexto los llamados "peñabots" hicieron

su primera aparición, si bien no la última.[14] Desde el apoyo al candidato del PRI, se entendió que las tendencias en redes sociales importan, pero que pueden ser alteradas y manipuladas. Es así que en respuesta al movimiento estudiantil, se desató una brigada de computadoras automatizadas para censurar a los estudiantes. Los "peñabots" son ejército de cuentas automatizadas en Twitter que se dedican a generar mensajes basura (*spam*) asociados a los *hashtags* tanto de organización como de protesta de los activistas mexicanos. Según la investigación de la periodista Erin Gallagher, son más de 75 mil máquinas de mensajes automatizados.[15] El propósito de los mismos es que los *hashtags* no lleguen a ser *trending topics*: al "contaminar" los mismos las etiquetas, el algoritmo de Twitter los elimina de la lista de tendencias destacadas.[16]

No obstante lo anterior, se realizaron decenas de marchas en más de cincuenta ciudades y se llegó a hablar de la "primavera mexicana" (Islas y Arribas, 2012). Pero, tal como sucede con las estaciones, el movimiento se extinguió. Enrique Peña Nieto ganó las elecciones con un cómodo margen de apoyo

14 Desde ese entonces, los "peñabots" han sido utilizados de manera habitual para alterar tendencias y manipular la opinión pública en redes sociales. Esta es una forma de represión que busca hundir la voz de la disidencia con ruido y manipulación mediática (Porup, 2015).

15 Erin Gallagher. "Mexican Botnets Dirty War". Ponencia en Chaos Communication Camp 2015, agosto de 2015, https://www.youtube.com/watch?v=13D3iIZGSt8 (Consultado el 11 de enero de 2016).

16 *Ibídem*.

popular y los medios de comunicación parecieron firmar un pacto silencioso con el poder en contra de la visibilidad de las voces críticas.

El PRI retomó, oficialmente, el poder político federal el primero de diciembre del año 2012. Su retorno trajo de regreso las memorias de casi 70 años de ejercicio autoritario del poder, el uso del ejército para la represión de protestas estudiantiles y la desaparición forzada de los disidentes.[17] Aquellos que se les opusieron durante las campañas se comprometieron a prevenir que dichas memorias se volvieran una realidad nacional de nueva cuenta, y ese mismo día las calles se inundaron para protestar, convocadas mediante redes sociales con el hashtag #1DMX y un sitio web asociado al movimiento.

La protesta callejera fue aplacada con la fuerza de policías especializados. Tal como lo narró con posterioridad la Comisión de los Derechos Humanos del Distrito Federal, "una cantidad considerable de personas –principalmente jóvenes– fueron víctimas de violaciones a sus derechos humanos derivadas de los cuestionables métodos y tácticas de

17 El escritor peruano y premio Nobel de literatura Mario Vargas Llosa llegó a calificar al gobierno del Partido Revolucionario Institucional como "la dictadura perfecta", por su habilidad de disfrazar sus prácticas de democráticas y su efectividad a la hora de encubrir sus crímenes. Ver Mario Vargas Llosa. "Vargas Llosa: 'México es la dictadura perfecta'". *El País*. 1 de septiembre de 1990. http://elpais.com/diario/1990/09/01/cultura/652140001_850215.html

respuesta a cargo de las autoridades locales y federales".[18] Se documentaron 32 detenciones arbitrarias y 20 heridos. Juan Francisco Kuykendall, herido por el impacto de balas de goma disparadas por la policía, murió un año después de los acontecimientos.[19]

Fuera de las calles, en marzo del 2014, la Embajada de Estados Unidos en México ordenó a GoDaddy –la empresa proveedora de dominios en internet más grande del mundo– que suspendiera la página asociada al movimiento #1DMX, www.1dmx.org, creada por el colectivo que se conformó después de los acontecimientos de ese primero de diciembre y que tenía como fin documentar los actos de represión y uso excesivo de la fuerza por parte de la policía durante manifestaciones. La empresa informó al colectivo que su página había sido suspendida por ser parte de una investigación policiaca.[20]

18 La recomendación 7/2013 de la Comisión de los Derechos Humanos del Distrito Federal, así como diversas intervenciones de los comisionados pueden consultarse en: http://cdhdfbeta.cdhdf.org.mx/tag/recomendacion-72013 y http://cdhdfbeta.cdhdf.org.mx/tag/informe-especial-1dmx (consultados el 11 de enero de 2016).

19 Fernando Camacho y Josefina Quintero. "Muere el activista Kuykendall, herido en el operativo policíaco del día 1 de diciembre de 2012", *La Jornada,* 26 de enero de 2014, http://www.jornada.unam.mx/2014/01/26/politica/011n1pol (consultado el 11 de enero de 2016).

20 Vladimir Garay, "La censura política en Internet es real: el caso de 1DMX.ORG", Derechos Digitales, 6 de marzo de 2014, https://www.derechosdigitales.org/7028/la-censura-politica-en-internet-es-real-el-caso-de-1dmx-org (consultado el 11 de enero de 2016).

La censura y la represión no terminó aquel día. Siguiendo el hábito descrito brevemente en estas líneas, la narrativa mediática de los sucesos se centró repetir que todo aquel que protestaba era delincuente y cometía actos criminales.[21] Yendo más allá, el gobierno reaccionó intentando tipificar conductas propias de la protesta y sometiendo a las nuevas manifestaciones públicas a una serie de requisitos burocráticos para su realización, con el efecto de desincentivarla o anularla.

2.3. La criminalización de la expresión de protesta

El 26 de septiembre de 2013, Miguel Ángel Mancera, gobernador de la Ciudad de México, dejó clara su línea política: "Quien ataque a la ciudad, encontrará la respuesta de la ley".[22] Al día siguiente presentó en la Asamblea Legislativa del Distrito Federal la iniciativa para reformar el artículo 287 del Código Penal con el fin de agravar el delito de "ultraje a la autoridad" si el mismo se cometía en contra de policías.[23] Pero el concepto mismo de "ultraje" es tan amplio, que

21 Esto se puede observar en algunas las portadas de los periódicos del día 2 de diciembre del año 2012 (un día después de los sucesos), como las recopiladas por Kiosko.net en esa fecha: http://kiosko.net/mx/2012-12-02/ (consultado el 11 de enero de 2016).

22 Alejandro Cruz. "Quien ataque a la ciudad encontrará la respuesta de la ley, advierte Mancera", *La Jornada,* 18 de septiembre de 2013, http://www.jornada.unam.mx/2013/09/18/capital/034n1cap (consultado el 11 de enero de 2016).

23 Asamblea Legislativa del Distrito Federal. "Presentan paquete de iniciativas de reformas al Código Penal para DF", 31 de octubre de 2013. http://www.aldf.gob.mx/comsoc-presentan-paquete-iniciativas-

permite la sanción con criterios subjetivos, por decir algo que las autoridades consideren ofensivo hacia los policías.

A nivel federal, se presentó el proyecto de Ley General de Regulación de Manifestaciones Públicas que tendría aplicación en todo el país. Se pretendía regular los derechos fundamentales de manifestación, asociación, reunión y tránsito. Establece limitación de horarios, exigencia de permisos, prohibiciones absolutas de utilizar vialidades primarias y un esquema de responsabilidad solidaria por presuntas infracciones cometidas durante protestas.[24] En la práctica, lo que hace es restringir el derecho a la libertad de reunión y a la libertad de expresión en el espacio físico al poner trabas y bloques barreras administrativos para ejercer el derecho a la protesta.

Por supuesto, las nuevas tecnologías usadas para esa protesta también quedarían cubiertas por el nuevo ánimo represor del gobierno. En julio de 2014, Enrique Peña Nieto presentó la iniciativa de ley denominada Ley Federal de Telecomunicaciones y Radiodifusión, también conocida como Ley Telecom. El texto inicial generó importantes reacciones negativas desde la sociedad civil, pues en su redacción original el proyecto de ley atentaba en contra del principio de neutralidad en la red y de libertad de información, al permitir en su

---

reformas-al-codigo-penal-df--15545.html (consultado el 11 de enero de 2016).

24 Gisela Pérez de Acha, "1º de diciembre: el gobierno que reprime las protestas", *Sin Embargo*, 1 de diciembre de 2013, http://www.sinembargo.mx/opinion/01-12-2013/19616 (consultado el 11 de enero de 2016).

artículo 145 que los concesionarios y autorizados pudieran "bloquear el acceso a determinados contenidos, aplicaciones o servicios a petición expresa del usuario, cuando medie orden de autoridad o sean contrarios a alguna normatividad".[25]

La vaguedad o ambigüedad del lenguaje legal se puede utilizar para actuar de manera injusta, aunque legal. En el caso de la Ley Telecom, la amplitud de la norma implicaba abrir la puerta al control y censura de internet por parte de empresas privadas. Si la neutralidad de la red impide que los proveedores de servicios de internet (como Telmex, Izzy o Axtel) perjudiquen o beneficien cierto tráfico sobre otro de manera arbitraria (por ejemplo, para beneficiar a un servicio de una de estas empresas o perjudicar a un competidor), esta iniciativa les permitía bloquear contenidos y expresiones que fueran en contra de sus intereses comerciales.[26]

Pero eso era solo el inicio. La Ley Telecom también proponía la posibilidad de "bloquear, inhibir o anular de manera temporal las señales de telecomunicaciones en eventos y lugares críticos para la seguridad pública y nacional a solicitud de las autoridades competentes". En pocas palabras, se abría la posibilidad para que en el marco de manifestaciones o protestas en espacios públicos -bajo un criterio laxo de seguridad pública- se pudieran bloquear las señales de internet y

25 Carlos Brito y Luis Fernando García, "Enrique Peña Nieto contra el internet", *Nexos*, 31 de marzo de 2014, http://www.redaccion.nexos.com.mx/?p=6176 (consultado el 11 de enero de 2016).

26 *Ibídem*.

telefonía. El efecto de una acción de esa naturaleza es enorme: incomunicar a quienes son parte de una manifestación pública no solamente deja sin capacidad de coordinación a quienes protestan, sino que los aísla de la capacidad de comunicarse con el resto de la población, sea para acusar actos de violencia, solicitar ayuda, o mostrar mediante registros gráficos lo que sucede en esos espacios públicos. Esto podría llevar a la confusión, desorganización y encubrimiento de prácticas violatorias de derechos humanos.

En el marco de protestas represivas, esto es de especial preocupación pues se impedirían esfuerzos de visibilización de la violencia policial. Un ejemplo de tales esfuerzos es la red #RompeElMiedo de la organización Artículo 19 (capítulo México) que busca, a través de mensajes identificados con ese *hashtag*, documentar el exceso de las fuerzas policiales y proponer rutas de evacuación segura en caso de persecución a quienes se manifiestan.[27]

Al final, y gracias a las movilizaciones sociales, ambas intenciones propuestas no prosperaron. Sin embargo, el resto de la Ley Telecom se promulgó y se convirtió en norma obligatoria. Los puntos clave no modificados fueron las nuevas reglas sobre vigilancia de las comunicaciones y el estado de concentración de medios de comunicación que existe en el país.[28]

27 Más información se encuentra en el sitio de Artículo 19 para la iniciativa #RompeElMiedo, http://rompeelmiedo.org/ (consultado el 11 de enero de 2016).

28 Para más información sobre el estado de vigilancia en México, véase el capítulo "La vigilancia y su impacto en el derecho a la privacidad

Los nuevos artículos 189 a 191 del proyecto de Ley Telecom, que ampliaban las facultades de localización geográfica en tiempo real de equipos de comunicación móvil, sin establecer un requisito previo –y mínimo– de orden judicial, quedaron vigentes. Estos se dirigen a quienes provean servicios de telecomunicaciones obligándolos "a prestar auxilio a las instituciones federales y locales de procuración de justicia", como las procuradurías federales y locales, policías ministeriales, ministerios públicos, el Consejo Nacional de Seguridad Pública, el CISEN, etcétera. En otras palabras, cualquiera de estas autoridades puede exigir a las empresas de telefonía que entregue información sobre la localización en tiempo real de sus usuarios: dónde están, a qué hora y con quién.

En el contexto de un país con la historia de represión que mantiene México, esto es sumamente preocupante, pues se puede utilizar como herramienta para el monitoreo y la disolución de reuniones y protestas sociales, además de su posible persecución penal, mediante la ubicación precisa de sus participantes. Un principio de vigilancia así de activo tiene un efecto silenciador sobre la disidencia: a cada movimiento rastreado, el miedo incrementa y las expresiones disminuyen.[29]

---

en México", de Luis Fernando García y Jesús Robles Maloof, en este mismo volumen.

29 Al momento de la elaboración de este artículo, continúa pendiente un proceso judicial ante la Suprema Corte de Justicia de la Nación, en contra de la legalidad dichas disposiciones, entablado por la Red en Defensa de los Derechos Digitales, junto a otras organizaciones y ciudadanos.

De forma más reciente, el proyecto de ley conocido como la Ley Fayad, presentado en octubre del año 2015 por el senador del PRI, Omar Fayad, buscó regular los delitos informáticos y la pornografía infantil. Sin embargo, lo hizo de manera tan laxa, tan amplia, que de haberse aprobado cualquier crítica y uso de redes sociales terminaría por criminalizarse.

Por ejemplo, "la difusión de información con el objetivo de causar pánico y desestabilización de la paz pública" contenida en el propuesto artículo tres; o una regulación excesiva del delito de intimidación en redes sociales a quien "acose, hostigue, intimide, agreda o profiera cualquier forma de maltrato físico, verbal o psicológico en contra de usuarios de internet, de forma reiterada y sistemática".[30] Al final, y gracias a la presión ejercida por la sociedad civil, la iniciativa tampoco prosperó.

Aunque los objetivos que persiguen estas leyes parezcan loables, es importante detectar zonas normativas que puedan abrir las puertas a la discrecionalidad de las autoridades y que puedan utilizarse como fundamento legal para censurar, silenciar e intimidar a la disidencia.

2.4. Ayotzinapa

La noche del 26 de septiembre de 2014, 43 estudiantes de la Escuela Normal Rural de Ayotzinapa desaparecieron en

30 Red en Defensa de los Derechos Digitales. "10 puntos clave sobre la #LeyFayad, la peor iniciativa de ley sobre Internet en la historia", R3D, 28 octubre de 2015, https://r3d.mx/2015/10/28/10-puntos-clave-sobre-la-leyfayad-la-peor-iniciativa-de-ley-sobre-internet-en-la-historia/ (consultado el 11 de enero de 2016).

manos de fuerzas de la policía municipal de Iguala, en el estado de Guerrero, después de protestar conmemorando la represión de Tlatelolco de 1968. Cuando la noticia de este secuestro y desaparición masiva llegó al público, surgió una nueva causa de lucha compartida por movimientos sociales muy distintos.[31] Diversos ecosistemas sociales se unieron bajo un mismo paraguas: el zapatismo, los estudiantes que protestaban por educación gratuita en la Universidad Nacional Autónoma de México en el año 1999, hasta el propio #YoSoy132.

El caso de los 43 de Ayotzinapa fue el punto de partida de nuevas reclamaciones en México y de movimientos sociales de apoyo en el resto de América Latina con un fuerte componente de uso de tecnologías, de lo que da cuenta en detalle Bernardo Gutiérrez (2015). Las expresiones de solidaridad se vieron en redes sociales desde movimientos tan variados como Yasunidos en Ecuador, las Madres de Mayo en Argentina y la hinchada del equipo de fútbol The Strongest en Bolivia. En Chile, estudiantes, madres y jugadores de fútbol realizaron un video relacionando Ayotzinapa con los desaparecidos de la dictadura, pidiendo al final "no más desaparecidos en América Latina". En Venezuela, Uruguay y Costa Rica también se dieron fuertes muestras de solidaridad. Para Gutiérrez, sin el precedente de #YoSoy132, un mo-

31 Para una línea de tiempo completa consultar: *Vice News*, "Ayotzinapa: A Timeline of the Mass Disappearance That Has Shaken Mexico", https://news.vice.com/article/ayotzinapa-a-timeline-of-the-mass-disappearance-that-has-shaken-mexico (consultado el 11 de enero de 2016).

vimiento social de la magnitud del que siguió a los sucesos de Ayotzinapa no hubiera sucedido.

Uno de los momentos más significativos de esa reclamación social ocurrió el viernes 7 de noviembre de 2014, cuando el procurador Jesús Murillo Karam, encargado de investigar la desaparición de los normalistas, durante una rueda de prensa reaccionó a las preguntas diciendo enérgicamente "ya me cansé". La frase se subvirtió para englobar el hartazgo del público mexicano sobre la sensación de impunidad de casos tan escandalosos como el de Ayotzinapa. Pronto, el *hashtag* #YaMeCansé se convirtió en tendencia global en Twitter.[32]

Esa misma noche apareció pintada la frase "#YaMeCansé del miedo", hecha por el colectivo Rexiste, afuera del edificio de la Procuraduría General de la República en la Ciudad de México.[33] Un día después, el *hashtag* se expandía a Estados Unidos, España e Inglaterra y llegaría a ser *trending topic* durante 26 días en todo elmundo. Pero como explica Gutiérrez (2015), el tres de diciembre el *hashtag* salió de los asuntos más hablados de Twitter, en parte por un ataque coordinado de 50 mil *bots* que seguían la misma lógica y actuaciones de quienes atacaron el movimiento #YoSoy132 en las redes du-

32 24 Horas. "#YaMeCansé: Frase de Murillo Karam se viraliza", 7 de noviembre de 2014, http://www.24-horas.mx/yamecanse-frase-de-murillo-karam-se-viraliza-vine/ (consultado el 11 de enero de 2016).

33 Rexiste. "Pinta "#YaMeCansé del miedo" en la PGR de Reforma, el día que el procurador se cansó", 7 de noviembre de 2014, http://rexiste.org/post/107241783217/pinta-yamecans%C3%A9-del-miedo-en-la-pgr-de-reforma (consultado el 11 de enero de 2016).

rante el año 2012. Surgieron así varios *hashtags* parelelos: de #YaMeCansé2 hasta #YaMeCanse27, manteniendo la cuestión de Ayotzinapa viva en las redes y los medios.[34]

Un año después de intensas marchas y exigencias por parte de la ciudadanía, no existía ninguna respuesta coherente a la desaparición de los normalistas. Pero el uso de mensajes en redes sociales con *hashtags* ha contribuido a la memoria de los sucesos ocurridos y sus víctimas y a que la tecnología sirva para mantener la indignación, aunque los medios de comunicación guarden cómplice silencio sobre esos hechos.

2.5. Nuevas formas de reprimir el disenso

Fuera de las calles y el terreno legal, existen también otros mecanismos de reprimir la protesta. En noviembre de 2014 el diario digital mexicano Sin Embargo fue víctima de dos ataques cibernéticos que limitaron el acceso a sus usuarios. El ataque fue confirmado como un DDoS y causó que el servicio fuera inaccesible a usuarios legítimos.

Los DDoS son, en esencia, muy sencillos. Parten de la premisa que un servidor de internet únicamente puede atender a un número finito de solicitudes. Si se envían solicitudes falsas y en grandes cantidades, la consecuencia es que se limita el acceso a recursos y servicios a otros usuarios. El despliegue de un DDoS causa la percepción que el servicio

34 *El Semanario*. "¿Por qué desapareció #YaMeCansé del Trending Topic de Twitter?", 4 de diciembre de 2014, http://elsemanario.com/83764/por-que-desaparecio-yamecanse-de-los-tt-de-twitter/ (consultado el 11 de enero de 2016).

es lento o no está disponible. Esto equivale muchas llamadas simultáneas: que miles de computadoras realicen solicitudes de manera simultánea para consumir todo el tiempo de respuesta del servidor y disminuir o eliminar su capacidad de respuesta. A grandes rasgos, los DDoS tratan de explotar una de las siguientes vulnerabilidades: el límite de ancho de banda, el límite de recursos computacionales o los límites en el diseño del software. Todos, con el fin de limitar el acceso a los sistemas bajo ataque (Shakarian, 2013).

El ataque a *Sin Embargo* duró varios días hasta que logró afectar el servidor. No pudo ser controlado por especialistas.[35] Aunque se pueda dudar de las motivaciones tras el ataque, Sin Embargo es un periódico digital que ha mantenido una línea editorial muy crítica de la administración de Enrique Peña Nieto.

Del mismo modo, el sitio de noticias Aristegui Noticias fue víctima de varios de este tipo de ataques después de revelar las ejecuciones extrajudiciales ocurridas en Apatzingán, Michoacán.[36] No existe ninguna evidencia de que el poder político haya orquestado dichos ataques, sin embargo, muchos activistas mexicanos encontraron en este

35 Redacción *Sin Embargo*. "SinEmbargo sufre el segundo ataque en un mes", 11 de noviembre 2017, *Sin Embargo*, http://www.sinembargo.mx/11-11-2014/1165773 (consultado 11 de febrero 2016).

36 Redacción *Aristegui Noticias*. "Atacan Aristegui Noticias; el sitio, caído varias horas", *Aristegui Noticias*, 19 de abril del 2015, http://aristeguinoticias.com/1904/mexico/atacan-aristegui-noticias-el-sitio-caido-varias-horas/ (consultado el 12 de febrero del 2016).

DDoS una afronta a la libertad de expresión de resultado favorable al gobierno.[37]

Un DDoS puede convertirse así en una herramienta para la censura y la represión del discurso opositor, que la ley toma como ataque informático digno de sanción. Pero por tratarse de una forma de ataque que no requiere autoridad, sino mera capacidad técnica, cabe entonces preguntarse si un ataque de esta naturaleza contra objetivos de un gobierno represor o de un adversario particular constituirían una forma legítima de protesta.

3. Propuestas de política pública

Frente a todo este contexto, ¿qué aproximación se debe tomar frente a la protesta para garantizar plenamente su ejercicio? ¿Qué estándares se deben seguir y qué conductas se deben evitar? ¿Cómo maximizar el derecho a la libertad de expresión en línea, para que también pueda servir a las protestas en el mundo real? El propósito de este ejercicio es trascender al análisis y hacer propuestas concretas de política pública en sustento al ejercicio de las libertades de expresión y de reunión, que se extienda al uso de herramientas de comunicación digital.

Para salir de los dilemas de una población atrapada entre el poder gubernamental y el poder de las grandes corpora-

37 Huellas de México. "Artículo 19 exige restaurar sitio de Aristegui, confirman ataque DDos", *Huellas*, 19 de abril del 2015, http://huellas.mx/nacional/2015/04/19/articulo-19-exige-restaurar-sitio-de-aristegui-confirman-ataque-ddos/ (consultado el 12 de febrero del 2016).

ciones privadas, la transparencia es necesaria: pensar en un gobierno líquido y digital, donde se cobren impuestos y se ejerza el gasto, mediado por un mecanismo eficaz para medir la opinión pública (esto es, la democracia) y donde la transparencia no sea un accesorio, sino una condición del sistema. Para lograrlo, debemos deshacernos de la idea de que el gobierno es una máquina de secretos que toma nuestro dinero y lo gasta en la oscuridad (Assange *et al*, 2013). El juego en el que estamos, divide al gobierno de los ciudadanos y nos obliga a jugar el papel de un detective que –poco a poco y con recursos asimétricos– tiene que desenterrar los cadáveres de la corrupción y el dispendio.

En un país donde las instituciones son fallidas, es difícil trazar directivas de política pública que vayan a cumplirse. Desafortunadamente, México se encuentra en el lugar más extremo del espectro: la criminalización de las distintas formas de protestas, por distintas vías legales o fácticas.

Sin embargo, tomando como base los principios que contiene la Declaración Conjunta sobre Libertad de Expresión e Internet hecha por tres relatores de libertad de expresión en el mundo, pueden dibujarse algunas respuestas.

Primero, hay que tener claro que el derecho a la libertad de expresión en relación con la protesta se aplica de la misma manera a internet que fuera de ella, aunque se deben atender las particularidades de este medio concreto. Entre otras, las posibles restricciones al ejercicio de la expresión en la red deben cumplir los estándares de la prueba tripartita: i) estar

especificadas en la ley, ii) perseguir una finalidad legítima reconocida por la Convención Americana sobre Derechos Humanos, es decir, que proteja los derechos de terceros, su reputación o la moral y el orden público, y iii) que sean necesarias para alcanzar dicha finalidad, o en otras palabras, que no impliquen mecanismos que restrinjan más derechos de los que efectivamente protegen.

Así, por ejemplo, en relación con la reciente Ley Fayad y sobre este último principio, debe tomarse en cuenta que al regular "delitos informáticos" debe tenerse mucho cuidado de valorar las implicaciones que los tipos penales pueden tener sobre el derecho a la libertad de expresión en internet, incluyendo la disidencia y los mecanismos de protesta.

La declaración conjunta de los relatores especiales de libertad de expresión de Naciones Unidas y de la OEA señala que los enfoques de reglamentación desarrollados para otros medios de comunicación –como telefonía o radio y televisión– no pueden transferirse sin más a internet, sino que deben ser diseñados específicamente para este medio, atendiendo a sus particularidades.[38] Una de las cosas más

38 Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), "Declaración Conjunta sobre Libertad de Expresión e Internet", 1 de junio de 2011,

relevantes a considerar dentro las particularidades de internet, es el concepto de la "responsabilidad de intermediarios", que se refiere a que nadie puede ser responsabilizado por expresiones de terceros. Esto incluye a empresas de internet como Twitter, Facebook o Google, que no deben ser forzadas a asumir responsabilidad por el contenido que se genere en sus plataformas. De otra manera, se crearían incentivos para que estas empresas censuren expresiones legítimas por miedo a incurrir en responsabilidades legales.

En todo caso, para remover o restringir contenidos de la red, proponemos la necesidad de una orden de una autoridad judicial y de estándares que sigan la lógica del debido proceso.

La Declaración Conjunta lo establece de la siguiente manera:

> Como mínimo, no se debería exigir a los intermediarios que controlen el contenido generado por usuarios y no deberían estar sujetos a normas extrajudiciales sobre cancelación de contenidos que no ofrezcan suficiente protección para la libertad de expresión (como sucede con muchas de las normas sobre "notificación y retirada" que se aplican actualmente).[39]

De manera muy importante, es obvio que el bloqueo de sitios web enteros o redes sociales es una medida extrema que no está justificada salvo en casos muy especiales y con las

---

https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849 (consultado el 11 de enero de 2016).

39 *Ibídem.*

debidas salvaguardas procesales. El gobierno no debe tener la capacidad de censurar sitios web de activistas que denuncian sus excesos, pues viola tanto la expresión de aquellos como el derecho de acceso a la información del resto de los internautas. Tal acción debe estar excluida de la potestad gubernamental, sino entregada a una autoridad judicial independiente e imparcial, mediando un procedimiento justo.

En cuanto al estándar de neutralidad en la red, y haciendo referencia a la Ley Telecom, una política pública adecuada debe tomar en cuenta que no se debe permitir que las empresas que proveen servicios de internet, discriminen el contenido y las expresiones que pasan por sus plataformas de manera arbitraria. Esto incluye la proscripción del *zero-rating*, allí donde los servicios gratuitos puedan implicar la promoción de plataformas donde la expresión es limitada. En todo caso, también deben ser transparentes con las prácticas que empleen para gestionar el tráfico.

En cuanto a la Ley Telecom, que buscaba dotar a las autoridades con la facultad para "bloquear" señales de telecomunicaciones en momentos determinados, la declaración conjunta es muy clara al decir que la interrupción del acceso a internet "no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional." Es decir, que en el marco de una protesta callejera, nada justifica que se impida el acceso a internet o partes del mismo.

En lo que se refiere a la protesta o el desafío a la autoridad mediante lo digital, es necesario mantener firmes los prin-

cipios constitucionales de defensa de la libertad expresión. Esto incluye a su vez la defensa frente a ataques a algunos de sus presupuestos, como la neutralidad de la red, la privacidad de las comunicaciones y el anonimato.[40]

Respecto de aquellos actos de protesta digital que van más allá de la expresión verbal o textual, como son los DDoS, creemos, como Sauter (2014), que bajo ciertas circunstancias estos ataques se producen como actos de expresión dignos de protección en lugar de sanción penal. Es decir, bajo ciertas condiciones, un ataque informático constituye un acto de protesta, tal como la ocupación de un edificio o la pintura de una consigna en un muro, que a su vez no merece una sanción penal.

Proponemos cuatro principios para la no penalización de esos ataques: temporalidad, proporcionalidad, legalidad y finalidad.

El primer se refiere a la limitación del ataque a un tiempo determinado, que no implique daños permanentes o irreparables, sino que se limite al objetivo de expresión. La proporcionalidad se refiere a su objetivo inmediato: un ataque legítimo sobre la web informativa de un banco, por ejemplo, no interrumpe ningún servicio crítico, a diferencia de un ataque que busca imposibilitar servicios críticos, afectando también a sus usuarios. En un ataque legítimo, el "daño" es mayor en un sentido simbólico que material. La legalidad, se refiere a

40 Si bien esos temas son de crucial importancia para la protesta social, ellos ya son examinados con detención por otros autores en el presente volumen, por lo que no se profundizan en este capítulo.

que el acto de protesta no debe producirse con vulneración de derechos fundamentales de otros. Por último, un criterio de finalidad: las causas que justifican la protesta se relacionan con los problemas y el malestar de la sociedad o de parte de ella. Su razón de ser no es promover deseos o convicciones de un solo individuo o grupo, sino el reconocimiento de intereses que la comunidad completa pueda considerar legítimos.

La legitimidad de la protesta social está vinculada a una cuestión no solo de participación, sino también de finalidad: el porqué de una protesta sí importa, y puede también hacerse un juicio de legitimidad sobre esa finalidad, por ejemplo, por su vinculación con derechos reconocidos en la Constitución. El fin de la protesta social, digital o no, es casi siempre el mismo: llamar la atención de la opinión pública y de quienes ejercen poder sobre un hecho o situación de relevancia social, y mostrar descontento frente a esa situación cuando lesiona intereses legítimos.

Reconocer esa legitimidad, a su vez, implica reconocer que los actos opuestos a esa protesta son ilegítimos, que deben ser prevenidos y combatidos. Esto requiere cambios en la legislación, pero también cambios políticos más profundos en que el poder político, económico y social deje de ver en el descontento una amenaza que aplastar. La defensa de la libertad de expresión y de la libertad de reunión para la protesta social es, en el fondo, la defensa de las vías de interacción que permiten la existencia de una sociedad democrática. Defender el disenso es defender la democracia.

4. Conclusiones

La protesta social y su represión son parte importante de la historia y el contexto mexicano. Ello se ha extendido al entorno digital, aunque ahí la protesta se encuentra aún en una etapa de infancia. Sin embargo, los intentos de los poderes mediáticos y políticos mexicanos por controlar internet (y así controlar las expresiones de descontento en la red), no han sido menores. Las interrogantes a nivel nacional e internacional son muchas y las respuestas pocas.

Es por esto que se debe insistir en lineamientos claros que fomenten y defiendan el derecho a la libertad de expresión y protesta en internet, sin caer en el reduccionismo de responsabilizar a empresas por el contenido de terceros en sus plataformas; o de utilizar mecanismos penales que, a pesar de tener objetivos legítimos, desincentivan la disidencia por la amplia gama de conductas que sancionan y por la vaguedad de los términos que utilizan (Ferrajoli, 2009).

La protesta en México, de marcado carácter político, denota que la democracia representativa parece cada vez más una simulación. Se trata de un acuerdo institucional que, tras largo tiempo sin reformas estructurales, ha convertido a las potestades gubernamentales en un botín al que solo puede accederse si se invierte muchísimo capital y al que se cuida aplacando a sus amenazas. Siempre que surge una nueva manera de protestar contra el poder, nace una nueva forma represión.

En este trabajo intentamos hacer un análisis de un nuevo régimen global donde las empresas y gobiernos tienen los me-

dios para reprimir. Ahí en medio está internet. Un bien que parece ser público y accesible a todos, pero que está gestionado por privados; que se utiliza, por igual, como medio de los que protestan y como medio para limitar esas expresiones.

Relatamos cómo en México el movimiento #YoSoy132 se gestó en redes sociales en el curso de las elecciones presidenciales de 2012, iniciando una continua práctica de identificar movimientos y protestas con un símbolo propio de las redes sociales digitales: el *hashtag*. La respuesta gubernamental ha sido una combinación entre represión policial directa y medidas violatorias de derechos fundamentales, incluyendo iniciativas de ley contra el principio de neutralidad en la red, hasta estrategias gubernamentales para incidir en los trending topics, también conocidas como "boteo" o "peñabots".

Nuestra conclusión es sencilla: la capacidad de controlar internet parece avanzar más rápido que los movimientos por asegurarla como espacio para el ejercicio de la protesta y la libre expresión. Un puñado de empresas controlan demasiados tramos donde la aparente libertad de internet se estrecha.[41] Retomar el control de la red por parte de quienes la necesitan para la información y la expresión, es un imperativo para la sociedad completa.

Al igual que la protesta fue una clave para las conquistas de la democracia liberal, el activismo digital es la pieza fundamen-

41 El Acuerdo Transpacífico de Cooperación Económica (TPP, por sus siglas en inglés), del que México es parte, es un buen ejemplo de cómo un puñado de empresas se están apoderando de los recursos del mundo y utilizando al Estado como su brazo ejecutor (Rimmer, 2015).

tal para la construcción de las democracias del futuro. Cerrarle la puerta, criminalizarla y reprimirla es un acto suicida.

Asamblea Legislativa del Distrito Federal, "presentan paquete de iniciativas de reformas al Código Penal para DF", 31 de octubre de 2013. http://www.aldf.gob.mx/comsoc-presentan-paquete-iniciativas-reformas-al-codigo-penal-df--15545.html (consultado el 11 de enero de 2016).

Brito, Carlos y Luis Fernando García. "Enrique Peña Nieto contra el internet", *Nexos*, 31 de marzo de 2014, http://www.redaccion.nexos.com.mx/?p=6176 (consultado el 11 de enero de 2016).

Cruz, Alejandro. "Quien ataque a la ciudad encontrará la respuesta de la ley, advierte Mancera". *La Jornada,* 18 de septiembre de 2013, http://www.jornada.unam.mx/2013/09/18/capital/034n1cap (consultado el 11 de enero de 2016).

De la Porta, Donatella y Mario Diani. S*ocial Movements, an introduction*. Malden, MA: BlackWell Publishing, 2006. http://www.hse.ru/data/2012/11/03/1249193172/Donatella_Della_Porta_Mario_Diani_Social_Mov.pdf

Dalton, Russell. *Citizen Politics: Public Opinion and Political Parties in Advanced Industrial Democracies*. Chatan, NJ: Sage Publications, 2008.

Ferrajoli, Luigi. *Derecho y razón*. España: Trotta, 2009.

Froheling, Oliver. "The Cyberspace 'War of Ink and Internet' in Chiapas, Mexico". *Geographical Review,* 87: 291–307. Nueva York: American Geographical Society, 1997. doi: 10.1111/j.1931-0846.1997.tb00076.x

Garay, Vladimir. "La censura política en Internet es real: el caso de 1DMX.ORG". Derechos Digitales, 6 de marzo de 2014. https://www.derechosdigitales.org/7028/la-censura-politica-en-internet-es-real-el-caso-de-1dmx-org (consultado el 11 de enero de 2016).

Gilly, Adolfo. "Memorias de una infamia. Atenco no se olvida". *La Jornada,* 9 de junio de 2012. http://www.jornada.unam.mx/2012/06/09/politica/013a1pol (consultado el 11 de enero de 2016).

Gutiérrez, Bernardo. "#Ayotzinapa: la expansión global de una causa". *Horizontal*, 25 de septiembre de 2015. http://horizontal.mx/ayotzinapa-la-expansion-global-de-una-causa/ (consultado el 11 de enero de 2016).

Halabi, Yakub. "Democracy, Clan Politics and Weak Governance: The case of the Arab municipalities in Israel". *Israel Studies*, vol. 19, no. 1. Indiana: Indiana University Press, 2014.

Hall, David. *Calvin in the public square. Liberal democracies, Rights and Civil Liberties*. Nueva Jersey: P&R Publishing, 2009.

Hernández, Luis. "The global zapatista movement", *Global*

Exchange, 16 de enero de 2004. http://www.globalexchange.org/news/global-zapatista-movement (consultado el 10 de enero de 2016).

Hobsbawm, Eric. *Fractured Times: Culture and Society in the Twentieth Century.* Nueva York: The New Press, 2009.

International Network of Civil Liberties Organizations. "Take Back the Streets. Repression of Protest and Criminalization Around the World". Nueva York: INCLO, 2013. https://www.aclu.org/files/assets/global_protest_suppression_report_inclo.pdf (consultado el 10 de enero de 2016).

Islas, Octavio y Amaia Arribas. "Enseñanza y ejemplo de la primavera mexicana". *Razón y Palabra* 80. Monterrey: Instituto Tecnológico y de Estudios Superiores de Monterrey, 2012.

Lane, Jill. "Digital Zapatistas". *TDR*, vol. 47, no. 2. Massachusetts: MIT Press, 2013.

Leigh, David. *Wikileaks: Inside Julian Assange's war on secrecy.* Estados Unidos: Public Affairs, 2011.

Marsden, Christopher. *Net neutrality: towards a co-regulatory solution.* Londres: Bloomsbury Academic, 2010.

Mancinas, Rosalba. "Concentración mediática en México: el caso del grupo Televisa". *Revista Synthesis* 42. Chihuahua: Universidad Autónoma de Chihuahua, 2008.

Muggah, Robert y Gustavo Diniz. "A new era of digital protest". *The Huffington Post,* 15 de octubre de 2013. http://www.huffingtonpost.com/robert-muggah/a-new-era-of-digital-protest_b_4089763.html (consultado el 11 de enero de 2016).

Pérez de Acha, Gisela. "1º de diciembre: el gobierno que reprime las protestas", *Sin Embargo,* 1 de diciembre de 2013. http://www.sinembargo.mx/opinion/01-12-2013/19616 (consultado el 11 de enero de 2016).

Porup, J.M. "Así es como los peñabots censuran a los disidentes en México", *Vice*, 25 de agosto de 2015. http://www.vice.com/es_mx/read/como-los-bots-de-twitter-censuran-a-los-disidentes-en-mexico (consultado el 10 de enero de 2016).

Ramlal, Satyan. "Political economic frameworks for assessing e-democracy and digital government". *Conference for e-democracy and open government*. Austria: Austrian Institute of Technology, 2014.

Reiher, Peter. *Internet denial of service: Attack and defense mechanisms.* Nueva Jersey: Prentice Hall, 2014.

Rimmer, Matthew. "The Trans-Pacific Partnership: Copyright Law, the Creative Industries, and Internet Freedom", *Medium,* 24 de agosto de 2015, https://medium.com/@DrRimmer/the-trans-pacific-partnership-copyright-law-the-creative-industries-and-internet-freedom-960254be7f33 (consultado el 11 de enero de 2016).

Rodríguez, Jacinto. "Por qué el 68 no se olvida", *Eme Equis*, 20 de septiembre de 2015. http://www.m-x.com.mx/2015-09-20/por-que-el-68-no-se-olvida/ (consultado el 10 de enero de 2016).

Rovira-Sancho, Guiomar. "Activismo mediático y criminalización de la protesta: medios y movimientos sociales en México". *Convergencia, Revista de Ciencias Sociales*, vol. 20, no. 61. Toluca: Universidad Autónoma del Estado de México, 2013.

Santoro, Wayne. "The civil rights movement and the right to vote: black protest, segregationist violence and the audience". *Social Forces,* vol. 86, no. 4. Oxford: Oxford University Press, 2008.

Sanders, James. "Chinese government linked to largest DDoS attack in GitHub history". *TechRepublic*, 3 de abril de 2015, http://www.techrepublic.com/article/chinese-government-linked-to-largest-ddos-attack-in-github-history/ (consultado el 10 de enero de 2016).

Sauter, Molly. *The coming swarm.* Londres: Bloomsbury Academic, 2014.

Shakarian, Paulo. *Introduction to cyber-warfare.* Massachusetts: Syngress, 2013.

La vigilancia y su impacto en el derecho a la privacidad en México

Luis Fernando García y Jesús Robles Maloof

En los últimos años ha prevalecido una narrativa que busca confrontar la privacidad con la seguridad. Se argumenta que los Estados deben –y pueden– vulnerar la primera con medidas cada vez más invasivas, para poder tener la segunda. Con base en este discurso, particularmente exitoso en México, los estados se han dotado de capacidades legales, institucionales y tecnológicas para facilitar la invasión de la privacidad.

Este esfuerzo por facilitar el monitoreo de las actividades de las personas no ha venido acompañado de medidas que permitan que los ciudadanos ejerzan un control sobre las autoridades con facultades potencialmente riesgosas para el derecho a la privacidad.

Dado que las medidas de vigilancia encubierta suponen, primero, un poder invasivo amplio y, segundo, que este poder es ejercido sin conocimiento de la persona afectada, los riesgos y las consecuencias del abuso de este tipo de medidas son particularmente graves.

Dado el contexto de crisis en materia de derechos humanos

por el que atraviesa México,[1] donde no es poco común que las autoridades encargadas de la seguridad de la ciudadanía sean precisamente las que cometen crímenes en contra de la población, la ausencia de controles democráticos a la vigilancia estatal es particularmente preocupante.

El discurso estatal de defensa de la vigilancia adquiere tintes propagandísticos cuando no ofrece evidencia pública sobre si el aumento de las capacidades de intrusión ha tenido efecto alguno en la seguridad de las personas. De esta forma, se crea un pernicioso círculo de opacidad que evita la rendición de cuentas y excluye a la vigilancia estatal del debate democrático. Este círculo se cierra con la excepciones creadas bajo la idea de seguridad nacional, que retrasa considerablemente el acceso a la información pública sobre adquisiciones, integración de los órganos responsables de la vigilancia, los protocolos, resultados y evaluaciones de las políticas y su implementación.

1 Varios organismos internacionales han dado cuenta de prácticas de violación sistemática de derechos humanos en México y han calificado la situación imperante en México como una crisis de derechos humanos. Ver, por ejemplo, Juan E. Méndez, *Informe del Relator Especial sobre la tortura y otros tratos o penas crueles, inhumanos o degradantes. Sobre su misión a México, 28 de diciembre de 2014,* A/HRC/28/68, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session28/Documents/A_HRC_28_68_Add_3_SPA.docx (consultado el 6 de enero de 2016); y Comisión Interamericana de Derechos Humanos, Observaciones Preliminares de la visita in loco de la CIDH a México, 2 de octubre de 2015, https://www.oas.org/es/cidh/prensa/comunicados/2015/112A.asp (consultado el 6 de enero de 2016).

1. Contexto de la vigilancia en México

1.1. Contexto político y desarrollo de las facultades de vigilancia

Tras los atentados del 11 de septiembre de 2001 en Estados Unidos, la prioridad de las relaciones entre el gobierno norteamericano y el mexicano se dirigió a la cooperación para la seguridad. En la misma década, el surgimiento de la "guerra contra las drogas"[2] como política de Estado, puso el énfasis en el uso de la fuerza para combatir tanto los crecientes flujos regionales de estupefacientes, como el de personas migrantes de Centro a Norteamérica.

Una de las estrategias de estrechamiento en la colaboración en materia de seguridad entre México y Estados Unidos es la "Iniciativa Mérida", acordada entre los gobiernos de ambos países en el año 2008. Uno de sus componentes estratégicos es la transferencia de tecnología para "combatir el crimen", la colaboración e intercambio de información de inteligencia y el incremento de las capacidades de vigilancia.[3]

2 Entendemos como "guerra contra las drogas" una política de seguridad basada en la fuerza militar y policial anunciada por el expresidente Felipe Calderón en 2009 (aunque con antecedentes por lo menos desde la década de 1970), que se propuso desarticular las organizaciones criminales llamadas "carteles del narco". En lo esencial, el actual gobierno mexicano sostiene dicha política. Véase Guerrero (2010).

3 Departamento de Estado, "Iniciativa Mérida", http://www.state.gov/j/inl/merida/c30128.htm; ver también el estudio del Congreso de Estados Unidos sobre el tema: https://www.hsdl.org/?view&did=752276 (consultado el 5 de enero de 2016).

Aunado a lo anterior, existe evidencia que el gobierno de los Estados Unidos se ha beneficiado de las medidas de vigilancia implementadas por su par mexicano. Por ejemplo, hay reportes de una colaboración e intercambio de inteligencia obtenida mediante vigilancia de comunicaciones por parte de agencias de ambos países,[4] y se ha revelado que la Agencia Nacional de Seguridad de Estados Unidos (NSA por sus siglas en inglés), como parte de su programa denominado MYSTIC, recolecta la totalidad de los metadatos de comunicaciones de usuarios en México.[5]

1.2. El derecho a la privacidad de las comunicaciones en México

El derecho a la privacidad de las comunicaciones se protege en el artículo 16 de la Constitución federal mexicana.[6] En

4 Brad Heath, "U.S. secretly tracked billions of calls for decades", *USA Today*, 8 de abril de 2015, http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/ (consultado el 5 de enero de 2016); y Jason Lauv, "The NSA has set up shop at the US embassy in México", Vice, 24 de febrero de 2014, https://www.vice.com/read/the-nsa-has-set-up-shop-at-the-us-embassy-in-mexico (consultado el 5 de enero de 2016).

5 Ryan Devereaux, Glenn Greenwald, Laura Poitras, "Data Pirates of the Caribbean: The NSA is recording every cell phone call in the Bahamas", *The Intercept*, 19 de mayo 2014, https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (consultado el 5 de enero de 2016).

6 Constitución Política de los Estados Unidos Mexicanos: "Artículo 16. (...) Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas,

específico, los párrafos duodécimo y decimotercero de dicho artículo, contemplan lo que ha sido caracterizado por los órganos de interpretación constitucional en México como el derecho a la inviolabilidad de las comunicaciones.

Según la Constitución, para que una intervención de comunicaciones esté justificada, se deben cumplir varios requisitos:

- En primer lugar, se establece que las únicas autoridades facultadas para llevar a cabo la intervención de comunicaciones privadas son: a) autoridades federales facultadas por una ley; y b) el titular del ministerio público de cada uno de los estados del país.

- En segundo lugar, se exige que las autoridades facultadas obtengan previamente una autorización de parte de un juez federal. Se demanda también que dicha autorización fije el tipo de intervención, los sujetos y la duración de la medida.

---

siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor".

- Por su parte, se establece que la intervención de comunicaciones privadas no puede ser autorizada en materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor. Por ello, este tipo de medidas se limitan exclusivamente a la materia penal, negando además cualquier valor probatorio a las comunicaciones privadas intervenidas ilegalmente.

- Finalmente, existe un mandato constitucional expreso para sancionar penalmente cualquier acto que atente contra la privacidad de las comunicaciones privadas.

La Suprema Corte de Justicia de México ha interpretado el artículo 16 de la Constitución de manera que la protección constitucional de las comunicaciones privadas incluye todas las formas existentes de comunicación y aquellas que sean fruto de la evolución tecnológica, incluidas las formas de comunicación a través de internet.[7]

Además, tanto la Suprema Corte como la Corte Interamericana de Derechos Humanos han señalado que el derecho a la privacidad protege tanto el contenido de las comunicaciones como a los "datos de tráfico de comunicaciones" o metadatos, es decir, datos como el registro de números marcados, la identidad de los comunicantes, la duración de la comunicación, los datos de localización geográfica o la dirección IP.[8]

7 Suprema Corte de Justicia de la Nación, Primera Sala, Amparo en Revisión 1621/2010 y Contradicción de Tesis 194/2012.

8 Suprema Corte de Justicia de la Nación, Primera Sala, Amparo en

En este sentido, la Suprema Corte de México ha considerado, por ejemplo, que el acceso y análisis de datos almacenados en un teléfono móvil, sin autorización judicial, es una violación al derecho a la inviolabilidad de las comunicaciones privadas.[9]

A su vez, la Suprema Corte de México ha señalado que en el momento en que se escucha, graba, almacena, lee o registra una comunicación privada sin el consentimiento de los interlocutores, se consuma la violación al derecho. Esto es con independencia que, con posterioridad, se difunda o no el contenido de la comunicación interceptada.[10]

Por ejemplo, un correo electrónico se considera interceptado –y por consiguiente se vulnera el derecho a la inviolabilidad de las comunicaciones– a partir del momento en que, sin autorización judicial o consentimiento del titular de una cuenta, se viola la clave personal de acceso (*password*), sin importar si se lee o no el contenido de los correos electrónicos.[11]

Revisión 1621/2010 y Contradicción de Tesis 194/2012; Corte IDH. Escher y otros vs. Brasil, Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 6 de julio de 2009, Serie C No. 200, párr. 114.

9 Suprema Corte de Justicia de la Nación, Primera Sala, Contradicción de Tesis 194/2012.

10 Suprema Corte de Justicia de la Nación, Primera Sala, Amparo en Revisión 1621/2010 y Contradicción de Tesis 194/2012.

11 Suprema Corte de Justicia de la Nación, Primera Sala, Amparo en Revisión 1621/2010.

Por otro lado, la protección constitucional a las comunicaciones, en cuanto a su ámbito temporal, se prolonga con posterioridad al momento en que la comunicación se produce. De esta forma, se encuentran igualmente prohibidas la eventual intervención de comunicaciones en tiempo real, así como aquellas posibles injerencias que se realizan con posterioridad en los soportes materiales que almacenan la comunicación.[12] Es decir, intervenir una llamada telefónica en tiempo real sin autorización judicial, es tan violatorio como acceder a un mensaje telefónico almacenado en la memoria del teléfono sin dicha autorización.

Si bien la Constitución y la jurisprudencia protegen ampliamente el derecho a la inviolabilidad de las comunicaciones, aún son escasos los precedentes en materia de vigilancia de estas, por lo que el contenido y alcance del derecho en cuestión aún se encuentra en disputa.

2. Marco legal e implementación de la vigilancia

Las leyes mexicanas contemplan la posibilidad que se lleve a cabo la vigilancia de comunicaciones privadas en tres circunstancias: a) la investigación de delitos; b) la prevención del delito; y c) la protección de la seguridad nacional. A continuación, se hace un breve resumen de la forma en que estas facultades se encuentran reguladas.

12 Suprema Corte de Justicia de la Nación, Primera Sala, Amparo en Revisión 1621/2010 y Contradicción de Tesis 194/2012.

2.1. Marco jurídico de la vigilancia de las comunicaciones para la procuración de justicia

En México, la investigación de los delitos le corresponde al Ministerio Público, el cual se encuentra organizado, a nivel federal, en una Procuraduría General de la República (pronto a transformarse en Fiscalía General de la República) y, a nivel estatal, en las procuradurías o fiscalías locales.

La Procuraduría General de la República (PGR) tiene facultades para la intervención de comunicaciones privadas en el Código Federal de Procedimientos Penales (CFPP). Sin embargo, este último y los códigos procesales penales de cada Estado serán reemplazados por un nuevo Código Nacional de Procedimientos Penales (CNPP), el cual se convertirá en el código único en materia procesal penal en todo el país a más tardar el 18 de junio de 2016.

El Código Federal, que aún se encuentra en vigor, señala en su artículo 278 bis que "[l]as empresas concesionarias y permisionarias del servicio de telecomunicaciones o de internet, estarán obligadas a colaborar con las autoridades para la obtención de [comunicaciones privadas] cuando así lo soliciten". Igualmente, el artículo 278 ter detalla el procedimiento a seguir para llevar a cabo la intervención de comunicaciones privadas. Se señala la necesidad de obtención de una autorización judicial, la cual será otorgada cuando "se constate la existencia de indicios suficientes que acrediten la probable responsabilidad en la comisión de delitos graves".

Este mismo código establece que la solicitud y, en su caso,

la autorización deben detallar aspectos de la intervención que se pretende llevar a cabo como: el fundamento legal, el razonamiento por el que se considera procedente, el tipo de comunicaciones, los sujetos y los lugares que serán intervenidos y el periodo durante el cual se llevarán a cabo las intervenciones, el cual no debe exceder los seis meses. Debe existir una verificación judicial periódica del cumplimiento de los términos de la autorización y en caso que se decrete el no ejercicio de la acción penal, las comunicaciones obtenidas deben ser presentadas ante el juez y ser destruidas en su presencia.

Además, el artículo 133 quáter del Código Federal establece que la PGR puede pedir a concesionarios de servicios de telecomunicaciones, es decir a las empresas de telefonía, los datos sobre localización geográfica de los equipos móviles de sus usuarios, en tiempo real y sin autorización judicial. Esto es siempre y cuando se trate de investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión o amenazas.

Este artículo se impugnó en la Acción de Inconstitucionalidad 32/2012, interpuesta por la Comisión Nacional de los Derechos Humanos. Sin embargo, una mayoría de la Suprema Corte de México consideró la práctica de localización como constitucional, en el entendimiento que la figura únicamente se facultaba para casos de emergencia, respecto de delitos específicos y siendo esta localización geográfica una medida efímera, es decir, que se agota en un mismo momento y no permite el monitoreo continuado de dichos datos de localización.

Por su parte, el nuevo Código de Procedimientos Penales que sustituirá al ahora vigente y será válido en cada estado del país, también contempla facultades de intervención de comunicaciones privadas. El artículo 291, por ejemplo, establece que la intervención de comunicaciones privadas debe realizarse únicamente con autorización judicial previa, e incluye tanto el contenido de las comunicaciones, como los metadatos, ya sea en tiempo real o se acceda a los datos después que la comunicación se haya llevado a cabo.

No obstante, este nuevo Código de Procedimientos Penales es menos claro que el antiguo en cuanto a la exigencia a la autoridad de demostrar ante el juez algún indicio que la persona intervenida ha participado en un hecho delictivo.

A su vez, en el artículo 303 del nuevo código persiste la posibilidad de monitoreo de la localización geográfica en tiempo real de dispositivos de comunicación sin autorización judicial, y se amplía esta posibilidad a cualquier investigación y no a una lista cerrada de delitos como lo establece el Código de Procedimientos Penales que, por ahora, sigue vigente. La constitucionalidad de dicho artículo será analizada en las acciones de inconstitucionalidad 10/2014 y 11/2014, interpuestas por la Comisión Nacional de los Derechos Humanos y el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).

Por otro lado, en el nuevo Código Nacional de Procedimientos Penales se incluye la posibilidad de ordenar la conservación de datos contenidos en redes, sistemas o equipos de informática, sin orden judicial. Además, tampoco se agregan

salvaguardas adecuadas como la supervisión por parte de una institución independiente, medidas de transparencia estadística que revelen datos sobre cuántas veces se utilizan las herramientas de vigilancia o mecanismos de notificación diferida al usuario afectado, es decir, que las personas afectadas sean avisadas, en algún momento, que alguna autoridad accedió a sus comunicaciones y otros datos personales.

En diciembre de 2014, el Senado de la República aprobó una reforma a los artículos 291 y 303 del nuevo Código de Procedimientos Penales, en la que se establecería de manera inequívoca la necesidad de autorización judicial federal para llevar a cabo la localización geográfica, en tiempo real, de equipos de comunicación móvil y el acceso a datos conservados por concesionarios de telecomunicaciones (como las empresas de telefonía) y proveedores de aplicaciones y servicios en internet (por ejemplo, Google, Facebook, Twitter). Dicha reforma aún requiere aprobación de la Cámara de Diputados, la cual se encuentra pendiente.[13]

Finalmente, la Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro adoptada en el año 2010,[14] y la Ley Federal contra la Delincuencia Organizada adoptada en el 2007,[15] también otorgan a la PGR la posibilidad

13 *Gaceta Parlamentaria de la Cámara de Diputados*, 10 de Diciembre de 2014.

14 *Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro*. Artículos 24 y 25.

15 *Ley Federal contra la Delincuencia Organizada*. Artículos 8 y 16 a 28.

de intervenir comunicaciones privadas, previa autorización judicial federal.

2.2. Marco jurídico de la vigilancia de las comunicaciones para la prevención del delito

En el año 2009 se expidió la Ley de la Policía Federal, la cual faculta a esta institución a llevar a cabo la intervención de comunicaciones privadas para la prevención de ciertos delitos.

El artículo 48 de la ley señala expresamente que la autorización judicial para la intervención de comunicaciones privadas podrá otorgarse "únicamente a solicitud del Comisionado General, cuando se constate la existencia de indicios suficientes que acrediten que se está organizando la comisión de [...]delitos" que se listan en el artículo 51 de la ley.

Además, el artículo 8 fracción XXVIII faculta a la Policía Federal a solicitar, previa autorización judicial, a los concesionarios, permisionarios, operadoras telefónicas y todas aquellas comercializadoras de servicios en materia de telecomunicaciones, cualquier información, incluyendo la georreferenciación[16] de los equipos de comunicación móvil en tiempo real, para fines de prevención del delito.

2.3. Marco jurídico de la vigilancia de las comunicaciones para la seguridad nacional

La Ley de Seguridad Nacional (LSN) otorga al Centro de Investigación y Seguridad Nacional (CISEN), la principal agen-

16 Por georreferenciación nos referimos a la localización geográfica de un equipo de comunicación.

cia de inteligencia en México, la facultad de intervenir comunicaciones privadas en casos de "amenaza inminente a la seguridad nacional". El artículo 5 de la misma define las amenazas a la seguridad nacional de manera sumamente amplia, por lo que los supuestos para llevar a cabo la intervención de comunicaciones privadas son igual de vagos e imprecisos.

No obstante que la Ley de Seguridad Nacional reconoce la necesidad de una autorización judicial federal para intervenir de comunicaciones privadas, no existen otras salvaguardas contra posibles abusos, como medidas de transparencia, notificación o supervisión independiente.

Por el contrario, el artículo 51 de la LSN restringe el acceso a la información de manera amplia, al establecer como información reservada: "aquella cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignen", así como "aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza".

De esta forma, dado que el concepto de "amenaza a la seguridad nacional" es definido de manera amplia y vaga en la ley, y que la naturaleza de la actividad que lleva a cabo el CISEN es principalmente preventiva, es decir, intenta evitar eventos futuros de realización incierta, existe un riesgo agravado de abuso en la utilización de las medidas de vigilancia.

2.4. Otras normas relevantes: Ley de Telecomunicaciones, Lineamientos de colaboración en materia de seguridad y justicia, Ley General de Transparencia y Código Penal Federal

Existen otras normas relevantes para vigilancia de comunicaciones, independientemente del fin para el cual se pretenda llevar a cabo.

Por ejemplo, la Ley Federal de Telecomunicaciones y Radiodifusión establece en su artículo 189 la obligación genérica de los concesionarios de telecomunicaciones, e incluso de los proveedores de servicios, aplicaciones y contenidos de "atender todo mandamiento por escrito, fundado y motivado de la autoridad competente", dentro de las cuales se mencionan "las instancias de seguridad y procuración de justicia" sin que se establezca claramente qué autoridades comprenden dichas categorías.

Este artículo ha sido considerado por varias autoridades, distintas a las ya reseñadas, como suficiente habilitación para utilizar herramientas de vigilancia de comunicaciones, sin la necesidad que dicha facultad esté detallada en otra ley.[17]

17 Por ejemplo, la Unidad de Inteligencia Financiera de la Secretaría de Hacienda y Crédito Público se considera a sí misma "instancia de seguridad" a partir del mencionado artículo 189 y de un instrumento que no constituye una ley formal y material, a saber, las "Bases de Colaboración que en el marco de la Seguridad Nacional celebran la Secretaría de Gobernación y la Secretaría de Hacienda y Crédito Público". También se ha revelado que el Instituto Nacional Electoral ha realizado solicitudes con base a la Ley de Telecomunicaciones (Zuckerman y Murray, 2015).

Por otro lado, el artículo 190 fracción I de esta misma ley, establece la obligación de concesionarios de "colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil". Esto supone la ampliación de las facultades de "geolocalización" a autoridades que hoy por hoy no tienen facultad en una ley habilitante como lo son las "instancias de seguridad" o las "instancias de administración de justicia", las cuales no se encuentran definidas ni en la LFTR, ni en otra ley.

El artículo 190 fracción II de la LFTR obliga a las empresas que prestan servicios de telefonía y acceso a internet a conservar por 24 meses una gran cantidad de metadatos de comunicaciones, por ejemplo, el nombre y domicilio del suscriptor, el origen y destino de cada comunicación, el tipo de comunicación, su fecha, hora y duración, los números que identifican a cada teléfono móvil y cada tarjeta SIM o chip, e incluso los datos de la ubicación geográfica del dispositivo.

A su vez, el artículo 190 fracción III de la LFTR establece la obligación de entregar los datos conservados a "las autoridades a que se refiere el artículo 189 de esta ley, que así lo requieran" dentro de las 48 horas siguientes a la solicitud. Como ha sido mencionado anteriormente, la figura de "instancias de seguridad" no se encuentra definida en la ley, además es notable que no se establece explícitamente la necesidad de autorización judicial para obtener dichos datos.

Lo anterior es particularmente preocupante pues, según da-

tos ofrecidos por las empresas de telefonía móvil,[18] en el año 2013 dichas empresas recibieron solicitudes para acceder al registro de datos de 117.262 números telefónicos de parte de procuradurías de justicia. La anterior cifra, que no incluye a otros concesionarios de telecomunicaciones ni a solicitudes provenientes de otras instancias de seguridad, revela la magnitud y alcance masivo de estas medidas de vigilancia.

Por su parte, el Instituto Federal de Telecomunicaciones (IFT) debe expedir los "Lineamientos de Colaboración en materia de Seguridad y Justicia", según lo señala la Ley Federal de Telecomunicaciones y Radiodifusión. En noviembre de 2014, el IFT publicó un anteproyecto de esa regulación, que si bien no subsana los vicios de constitucionalidad de la ley, reconoce algunas salvaguardas en materia de transparencia. En concreto, el IFT obligaría a las empresas que prestan el servicio de telefonía y de acceso a internet a emitir un informe semestral de transparencia con estadísticas respecto del número de requerimientos recibidos, cumplidos y rechazados por autoridad solicitante.

En un sentido similar, la Ley General de Transparencia y Acceso a la Información Pública recientemente adoptada, obliga a todas la autoridades a poner a disposición del público y mantener actualizada, para efectos estadísticos, el listado de

18 ANATEL y Consejo Ciudadano Ciudad de México, "Estudio e Investigación para el Desarrollo de Nuevas Medidas Tecnológicas que Permiten Inhibir y Combatir la Utilización de Equipos de Telecomunicaciones para la Comisión de Delitos", 2014, http://www.anatel.org.mx/Estudio_seguridad_2014.pdf (consultado el 5 de enero de 2016).

solicitudes a empresas para la intervención de comunicaciones privadas, el acceso a los metadatos de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, incluyendo los fundamentos legales, la temporalidad, el objeto y la mención de si dicha solicitud cuenta con autorización judicial.

El Código Penal Federal, por su parte, contempla sanciones severas por invasión de las comunicaciones privadas. El artículo 177 impone una pena de seis a doce años de prisión a quien intervenga comunicaciones privadas sin mandato de autoridad judicial. Asimismo, en los artículos 211 a 211 bis 7 se establecen penas severas por el acceso ilícito a sistemas y equipos de informática.

2.5. Vigilancia ilegal

Las leyes que rigen la vigilancia de las comunicaciones en México no contemplan suficientes medidas para detectar e inhibir el abuso de las mismas. Como consecuencia, es difícil evaluar el cumplimiento y eficacia de la vigilancia para la consecución de los fines perseguidos. De cualquier manera, existe evidencia de prácticas de vigilancia ilegal que de manera generalizada permanecen en la impunidad.

El 5 de julio de 2015 se publicaron documentos internos de la empresa italiana Hacking Team, revelando que numerosas autoridades mexicanas, federales y estatales han adquirido software malicioso de espionaje (Angel, 2015a), la mayoría de ellas sin que posean facultades constitucionales o legales para intervenir comunicaciones privadas (Angel, 2015b).

Hacking Team tiene en México a su mejor cliente en el mundo, pues es el país que le representa mayores ganancias y donde se concentran la mayor cantidad de clientes vigentes o potenciales (Angel, 2015a).

Dentro de las autoridades que figuran como clientes de Hacking Team, se encuentran instancias como la Secretaría de Planeación y Finanzas de Baja California, la Secretaría de Gobierno de Jalisco, las oficinas de los gobernadores de Querétaro y Puebla, e incluso empresas estatales como PEMEX (Angel, 2015a). Dichas autoridades no poseen facultades constitucionales o legales para llevar a cabo la intervención de comunicaciones privadas, por lo que la contratación y uso del software y equipo comercializado por Hacking Team, a través de empresas intermediarias en México, es abiertamente ilegal.

Adicionalmente, fue revelado que la Secretaría de Defensa Nacional sostenía conversaciones para adquirir el software de Hacking Team denominado Pegasus. Según documentos revelados, el ejército mexicano buscaba obtener la capacidad para infectar y espiar a 600 objetivos de manera simultánea (Angel, 2015b), a pesar de que el ejército no posee facultad legal alguna para llevar a cabo la intervención de comunicaciones privadas de la población civil.

Debe señalarse que Hacking Team no es la única empresa que comercializa este tipo de software malicioso de espionaje en México. Existe evidencia que Gamma Group ha vendido licencias de uso del software denominado FinFisher, a través de empresas intermediarias a entidades federales como

la Procuraduría General de la República, la Policía Federal y el Estado Mayor Presidencial (Molina y Miguel, 2013), e incluso el Auditor Superior de la Federación ha detectado indicios de su venta al gobierno de Coahuila.[19]

El software malicioso de espionaje comercializado por estas empresas permite a autoridades infectar un dispositivo y controlar sus funciones básicas, de manera que se registre y envíe no solo la información y comunicaciones que se lleven a cabo a través del dispositivo, sino que también permiten la activación subrepticia de la cámara de video o el micrófono del dispositivo para registrar mayor información, la cual es automáticamente enviada a un servidor controlado por la autoridad para su análisis.

Dada la intensidad de la invasión a la privacidad que supone este tipo de software y la dificultad de su detección, es vital que existan contrapesos institucionales para fiscalizar su utilización y así impedir el abuso de dichas medidas.

Es importante señalar que el abuso de este tipo de vigilancia no es hipotético, pues se ha demostrado que autoridades como el Gobierno del Estado de Puebla han utilizado el software adquirido a Hacking Team para espiar a adversarios políticos (Aroche, 2015a). Además, existen fuertes indicios que periodistas también habrían sido objetivos de este tipo de vigilancia (Aroche, 2015b). En ningún caso se ha llevado

19 Informe del Resultado de la Fiscalización Superior de la Cuenta Pública 2010, Observación 32, http://www.asf.gob.mx/trans/Informes/IR2010i/Grupos/Gasto_Federalizado/2010_0293_a.pdf (consultado el 5 de enero de 2016).

a cabo una investigación seria e imparcial que haya concluído con la imposición de sanciones para persona alguna.

En conclusión, las deficiencias regulatorias, la proliferación de equipo y software de vigilancia altamente sofisticado por parte de autoridades sin facultades legales para utilizarlo, la evidencia que este software ha sido utilizado para fines ilegítimos en contra de las personas y la impunidad ante la vigilancia ilegal, demuestran que en México el derecho a la privacidad se encuentra seriamente amenazado.

3. Deficiencias regulatorias y amenazas al derecho a la privacidad

3.1. Vaguedad respecto de autoridades facultadas y circunstancias en las que se pueden llevar a cabo medidas de vigilancia

La legislación no señala con precisión la identidad de las autoridades facultadas para llevar a cabo medidas de vigilancia. En particular, la Ley Federal de Telecomunicaciones y Radiodifusión no es clara respecto a qué autoridades pueden implementar medidas como la localización geográfica en tiempo real de dispositivos de comunicación o el acceso a metadatos de comunicaciones conservados por las empresas de telecomunicaciones. Esta falta de certeza produce que autoridades que no poseen una facultad constitucional o legal expresa (como la Secretaría de Hacienda, el Instituto Nacional Electoral o los cuerpos de seguridad estatales o municipales), actúen como si tuvieran esa facultad, lo cual compromete la privacidad de los ciudadanos y la adecuada fiscalización de sus actividades.

Por otro lado, existen autoridades que sin duda poseen facul-

tades de intervención de comunicaciones privadas (como el Ministerio Público Federal y los ministerios públicos locales, el CISEN o la Policía Federal), pero la legislación que regula sus actividades no establece con precisión las circunstancias en las que pueden hacer uso de las mismas. Por ejemplo, la Ley de Seguridad Nacional es sumamente amplia en su concepción de "amenaza a la seguridad nacional", lo cual abre la puerta a un uso indiscriminado o indebido de las medidas de vigilancia. Igualmente, dada que la finalidad de las facultades de vigilancia otorgadas a la Policía Federal es la de prevenir conductas delictivas –es decir, prevenir actos futuros– persiste el riesgo de que las medidas de prevención sean utilizadas de manera discrecional para realizar una vigilancia generalizada o sobre personas respecto de las cuales no existe indicio alguno de su posible participación en actos preparatorios para la comisión de delitos.

En el caso de las instancias de procuración de justicia, el nuevo Código Nacional de Procedimientos Penales es menos claro respecto a la necesidad que existan datos que involucren a una persona en la comisión de un delito para que la autoridad judicial federal pueda autorizar la medida de vigilancia. Igualmente, la nueva legislación procesal penal otorga menor claridad respecto de las circunstancias en las que puede solicitarse la localización geográfica, en tiempo real, de dispositivos de comunicación, pues a diferencia del Código Federal de Procedimientos Penales, que establecía una lista cerrada de delitos cuya investigación facultaba la medida, el nuevo Código Nacional de Procedimiento Penales abre la puerta a su utilización en cualquier averiguación previa.

3.2. Ausencia de claridad de métodos de colaboración entre autoridades y empresas

Diversas disposiciones establecen a empresas de telecomunicaciones e incluso a compañías que proveen servicios en internet obligaciones de colaboración amplias y vagas. Es el caso del artículo 189 de la LFTR o el artículo 301 del CNPP, los cuales hacen exigencias genéricas, incluso de carácter técnico, para facilitar la vigilancia de comunicaciones. La vaguedad del lenguaje de dichas disposiciones abre la puerta a requerimientos de parte de la autoridad para facilitar la vigilancia que pueden vulnerar la integridad y seguridad de sistemas de comunicación.

3.3. Conservación indiscriminada y masiva de datos

La conservación indiscriminada y masiva de datos de usuarios de telecomunicaciones, como las que contempla el artículo 190 fracción II de la LFTR, atenta de manera severa con el derecho a la privacidad.

No solamente la acumulación innecesaria de la inmensa mayoría de los datos de los usuarios de telecomunicaciones, respecto de los cuales no existe dato alguno o sospecha de participación en un hecho delictivo o en una amenaza a la seguridad nacional, resulta altamente riesgosa para la privacidad, sino que ni siquiera se ha demostrado su efectividad y, por ende, no resulta una medida necesaria ni proporcional para la consecución de fines legítimos.

Este tipo de obligaciones de conservación de datos han sido declaradas contrarias al derecho a la privacidad por diversos

tribunales constitucionales y por el Tribunal de Justicia de la Unión Europea.[20] Además, existe evidencia que la ausencia de obligaciones de conservación indiscriminada de datos no obstaculizan la actuación de autoridades para la persecución del crimen o la protección a la seguridad nacional.[21]

Por todo lo anterior, es indispensable que en México se eliminen las obligaciones de conservación de datos contenidas en la LFTR.

3.4. Falta de claridad respecto de la necesidad de control judicial previo

El artículo 16 de la Constitución es claro al establecer la necesidad de una autorización judicial federal para llevar a cabo la intervención de comunicaciones privadas. Además, tanto la interpretación constitucional como la Ley de la Policía Federal y el Código Nacional de Procedimientos Penales son claros al establecer que la intervención de comunicaciones privadas comprende el acceso a metadatos y no solo al contenido.

20 Digital Rights Ireland, Seitlinger y otros, "Asuntos acumulados C-293/12 y C-594/12", comunicado de prensa del Tribunal de Justicia de la Unión Europea, 8 de abril de 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf (consultado el 5 de enero de 2016).

21 Por ejemplo, estudios independientes en Alemania (MPI, 2008) y Países Bajos (EUR, 2005), donde la retención de datos ha sido declarada inconstitucional, han confirmado que la ausencia de una obligación de conservación indiscriminada de datos de tráfico de comunicaciones no han impedido el acceso a los datos solicitados por las autoridades prácticamente ninguna investigación.

No obstante, persisten normas e interpretaciones que no reconocen explícitamente la necesidad del control judicial para llevar a cabo medidas de vigilancia encubierta, como el acceso a metadatos o la localización geográfica en tiempo real de equipos de comunicación.

Por ejemplo, la Ley Federal de Telecomunicaciones y Radiodifusión no establece explícitamente la necesidad de autorización judicial federal para el acceso a datos conservados o para la localización geográfica, en tiempo real, de dispositivos de comunicación. Inclusive, un juzgado federal[22] ha interpretado que, de hecho, el acceso a datos conservados no requiere de una autorización judicial.

Asimismo, el Código Nacional de Procedimientos Penales tampoco reconoce el control judicial previo o inmediato como requisito para llevar a cabo la localización geográfica, en tiempo real, de dispositivos de comunicación.

Dado que las medidas de vigilancia encubierta son, por naturaleza, secretas para la persona afectada, la ausencia de un control judicial previo o inmediato impide que exista un contrapeso institucional mínimo capaz de detectar e impedir el abuso de las medidas de vigilancia. Por ello, al no reconocerse explícitamente la necesidad de un control judicial previo o inmediato de dichas medidas, se vulnera de manera grave el derecho a la privacidad.

22 Específicamente, el Juzgado Segundo de Distrito en Materia Administrativa Especializada en Competencia Económica, Radiodifusión y Telecomunicaciones, con residencia en el Distrito Federal.

3.5. Ausencia de salvaguardas para la detección de usos ilegales de vigilancia: notificación, supervisión independiente y protección a denunciantes

Las medidas de control judicial no son suficientes para inhibir y detectar instancias de abuso de vigilancia. Por ello se ha entendido que es necesario que se adopten otras salvaguardas contra el abuso.

Una primera medida es la notificación posterior a la persona afectada por medidas de vigilancia, es decir, el derecho de toda persona a ser notificado de haber sido sujeto de una invasión a su privacidad, ha sido reconocida como una medida útil para la rendición de cuentas y la detección de abusos en materia de vigilancia de comunicaciones.

El Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas ha señalado al respecto que:

> Los individuos deben contar con el derecho a ser notificados que han sido sujetos de medidas de vigilancia de sus comunicaciones o que sus comunicaciones han sido accesadas por el Estado. Reconociendo que la notificación previa o concurrente puede poner en riesgo la efectividad de la vigilancia, los individuos deben ser notificados, en cualquier caso, una vez que la vigilancia ha sido completada y se cuenta con la posibilidad de buscar la reparación que proceda respecto del uso de medidas de vigilancia de las comunicaciones.[23]

23 Frank La Rue, "Informe del Relator Especial sobre el derecho a la

Este derecho de notificación ha sido reconocido además por el Tribunal Europeo de Derechos Humanos, el cual determinó en el Caso Ekimdzhiev vs. Bulgaria, que una vez que la vigilancia ha cesado y ha transcurrido el tiempo estrictamente necesario para que el propósito legítimo de la vigilancia no sea puesto en riesgo, la notificación al afectado debe llevarse a cabo sin dilación.[24]

Una segunda medida para incrementar la rendición de cuentas por el uso de herramientas de vigilancia es la existencia de un órgano de supervisión independiente. Por ejemplo, en la resolución "El derecho a la privacidad en la era digital", adoptada por consenso por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013, se recomienda a los Estados establecer o mantener "mecanismos nacionales de supervisión independiente y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado".[25]

---

libertad de opinión y expresión de la Organización de las Naciones Unidas", 17 de abril de 2013, A/HRC/23/40, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (consultado el 5 de enero de 2016).

24 TEDH, Caso de la Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev vs. Bulgaria, Aplicación Nº 62540/00, Sentencia de 28 de Junio de 2007.

25 Asamblea General de la **ONU**, "Resolución aprobada por la Asamblea General el 18 de diciembre de 2013. 68/167. El derecho a la privacidad en la era digital", A/RES/68/167, 21 de enero de 2014.

En México no existe un órgano independiente con las características descritas en el párrafo anterior. Si bien el Instituto Nacional de Acceso a la Información y Protección de Datos (INAI) posee algunas facultades para la protección de la privacidad, no tiene un mandato ni procedimientos expresos para supervisar de manera periódica la forma en la que las autoridades llevan a cabo medidas de vigilancia.

Igualmente, en años recientes se ha comprobado como, ante la ausencia de mecanismos institucionales para la detección y sanción de injerencias abusivas en la privacidad de las personas por parte de autoridades, la filtración de información se ha convertido en una herramienta indispensable para conocer dichos abusos y rendir cuentas a la autoridad. No obstante, en México no existe una protección legal específica para las personas que denuncian violaciones a derechos humanos y otras conductas ilegales, incumpliendo un deber de secrecía (*whistleblowers*) que desincentiva la transparencia y rendición de cuentas por este tipo de abusos.

3.6. Falta de transparencia

La transparencia es indispensable para que la ciudadanía pueda ejercer un control político sobre instituciones a las cuales le son otorgadas facultades tan invasivas como las de vigilancia de comunicaciones.

En este sentido, el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas ha expresado en su informe las consecuencias

de la vigilancia de las comunicaciones.[26] Así también lo ha hecho la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana sobre Derechos Humanos[27] que ha exaltado la importancia de las medidas de transparencia en reiteradas ocasiones.

Otro instrumento que reconoce la obligación de los Estados de garantizar la transparencia respecto de programas de vigilancia para fines de seguridad nacional son los Principios Globales sobre Seguridad Nacional y Derecho a la Información (Principios de Tshwane, en particular el Principio 10.E).[28]

Si bien existen avances en materia de transparencia, como el artículo 70 fracción XLVII de la Ley General de Transparencia,

26 Frank La Rue, obra citada.

27 Relator Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humano, "Declaración Conjunta sobre Programas de Vigilancia y su Impacto para la Libertad de Expresión" .21 de junio de 2013, http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2 (consultado el 5 de enero de 2016), y CIDH, Relatoría Especial para la Libertad de Expresión. "Libertad de Expresión e Internet". 31 de diciembre de 2013. OEA/Ser.L/V/II http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf (consultado el 5 de enero de 2016).

28 Principios Globales sobre Seguridad Nacional y el Derecho a la Información ("Principios de Tshwane") concluidos en Tshwane, Sudáfrica y emitidos el 12 de junio de 2013, https://www.aclu.org/sites/default/files/assets/spanish-version_of_the_tshwane_principles.doc (consultado el 5 de enero de 2016).

dicha disposición aún no ha sido trasladada a la Ley Federal de la materia ni a la legislación de transparencia de las entidades federativas. Asimismo, aún se encuentra pendiente la emisión de los lineamientos en materia de colaboración con instancias de seguridad y justicia por parte del IFT. Por lo tanto, en este momento aún no se han implementado las obligaciones de transparencia contempladas en el anteproyecto.

3.7. Impunidad ante ejercicios abusivos de vigilancia

Aun cuando, debido a la ausencia de contrapesos institucionales a la vigilancia estatal, es sumamente difícil la detección de instancias de abuso, existen evidencias de contratación y uso ilegal de la vigilancia por parte de diversas instituciones en México. No obstante, en ningún caso ha existido una investigación y sanción de los responsables.

La impunidad prevaleciente no solo incentiva la repetición de estas conductas, sino que agrava y socializa las consecuencias negativas de la vigilancia al generar sensaciones de indefensión ante la misma. La perpetuidad de esta dinámica tiende a producir procesos de normalización que pueden comprometer las aspiraciones democráticas de cualquier sociedad.

4. Soluciones y propuestas

En atención a la problemática identificada, es indispensable modificar las leyes existentes para hacerlas compatibles con las obligaciones de derechos humanos de México.

A continuación, se formulan diversas propuestas que pueden implicar una reforma a las múltiples leyes en las cuales se contemplan disposiciones de vigilancia de comunica-

ciones o, en su defecto, se propone la creación de una Ley General sobre la protección de la privacidad de las comunicaciones que regule todas las actividades de vigilancia del Estado, tanto a nivel federal como local.

4.1. Eliminación de obligaciones de conservación de datos

Se propone la eliminación del artículo 190 fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión, de manera que sea eliminada la obligación de parte de los concesionarios de telecomunicaciones de conservar, masiva e indiscriminadamente, datos de tráfico de comunicaciones de la totalidad de los usuarios de sus servicios.

Adicionalmente, deberían modificarse las disposiciones pertinentes, en particular el artículo 301 del CNPP, para establecer la facultad de las autoridades de procuración de justicia de solicitar, previa autorización judicial federal, la conservación de datos de un usuario determinado respecto del cual exista una sospecha razonable (causa probable) de que esté relacionado con la comisión de un delito grave.

En su caso, la autorización respectiva tiene que señalar con precisión la temporalidad de la conservación, debe existir una revisión periódica de las circunstancias que dieron origen a la orden de conservación y, en cualquier caso, debe garantizarse la transparencia del proceso y el derecho de notificación del usuario afectado.

4.2. Control judicial previo o inmediato de acceso a contenido o metadatos de comunicaciones a través de regulación de mecanismos de emergencia

La Ley General propuesta, o cualquier otra ley en su defecto, deben ser modificadas para establecer de manera explícita e inequívoca la necesidad de obtener una autorización judicial federal de manera previa a la intervención de comunicaciones privadas, incluyendo el acceso a metadatos de comunicaciones y la obtención de datos de localización geográfica en tiempo real.

Solamente en casos de emergencia, claramente definidos en la ley, debe permitirse el acceso a datos conservados o la localización geográfica, en tiempo real, de dispositivos de comunicación sin autorización judicial previa. Sin embargo, en los casos de emergencia, la solicitud de colaboración que sea enviada a la empresa correspondiente deberá realizarse de manera simultánea a la solicitud de autorización judicial.

La autorización que en su caso sea otorgada por la autoridad judicial federal tendrá efectos retroactivos, de manera que se entenderá que la medida fue autorizada desde un principio. En caso que la autoridad judicial niegue la autorización, se ordenará el cese de la medida, la destrucción de la información obtenida y se impondrán las responsabilidades que correspondan.

4.3. Establecimiento de derecho de notificación

Debe reconocerse y reglamentarse en las leyes el derecho de notificación a personas afectadas por medidas de vigilancia. De esta forma, toda persona cuyas comunicaciones u otros datos personales hayan sido obtenidos por una au-

toridad debe ser notificada de ello en el primer momento que sea posible.

El juez que haya autorizado la medida de vigilancia podrá diferir la notificación únicamente cuando la misma ponga en riesgo la consecución un interés legítimo, como lo puede ser la efectividad de una investigación o la protección de la seguridad nacional. En todo caso, la ley debe fijar plazos máximos para el diferimiento de la notificación.

4.4. Supervisión independiente

La ley debe otorgar facultades de supervisión de las medidas de vigilancia de comunicaciones al Instituto Nacional de Acceso a la Información y Protección de Datos, o a otro organismos independiente creado para ese efecto.

El instituto o el organismo, según sea el caso, debe poseer los recursos materiales y humanos para llevar a cabo su labor de manera independiente y autónoma. Asimismo, debe contar con facultades para acceder a toda la información que sea relevante para llevar a cabo su labor, incluyendo el acceso y revisión aleatoria de expedientes.

El mecanismo de supervisión debe publicar y difundir ampliamente los hallazgos producto del cumplimiento de sus obligaciones y debe estar facultado para imponer sanciones o, en su defecto, para iniciar procedimientos sancionatorios por el abuso de las medidas de vigilancia.

4.5. Protección legal a denunciantes

La ley debe reconocer la inmunidad de las personas que, de bue-

na fe, denuncien la violación de la ley, actos de corrupción o violaciones a derechos humanos en incumplimiento de un deber de secrecía. Esta inmunidad debe estar explícitamente reconocida en la legislación que impone sanciones penales o administrativas por el incumplimiento de estos deberes de secrecía.

4.6. Transparencia

La Ley Federal de Transparencia y Acceso a la Información Pública, así como las leyes de las entidades federativas en la materia, deben establecer, de igual manera a como lo señala la Ley General, la obligación de toda autoridad de hacer disponible públicamente en las páginas de internet de cada dependencia, sin que sea necesario que medie solicitud, información estadística respecto de las solicitudes de intervención de comunicaciones privadas, de acceso a datos conservados y de localización geográfica, en tiempo real, de dispositivos de comunicación.

De esta manera, como mínimo, debe establecerse la obligación de parte de las autoridades de seguridad y procuración de justicia, así como de los jueces de control, de publicar información estadística que permita conocer el número de solicitudes realizadas por autoridad, el objeto de la solicitud, el tipo de medida de vigilancia solicitada y autorizada, la empresa destinataria, el fundamento legal, así como el número de solicitudes autorizadas y negadas por la autoridad judicial federal.

En el caso de las autoridades de procuración de justicia, debe además indicarse información estadística respecto del esta-

do de las averiguaciones previas en las que se ha utilizado una herramienta de vigilancia. Lo anterior permite evaluar la efectividad de este tipo de medidas.

Por otro lado, los "Lineamientos de Colaboración en materia de Seguridad y Justicia" que debe emitir el IFT deben establecer obligaciones a las empresas concesionarias y autorizadas para prestar servicios de telecomunicaciones de publicar informes de transparencia periódicos que permitan conocer información estadística respecto del número de solicitudes recibidas por autoridad, tipo de medida y objetivo. Igualmente, debe informarse el número de solicitudes cumplidas y rechazadas, así como el motivo de rechazo o si alguna solicitud ha sido combatida judicialmente.

4.7. Investigación y sanción de responsables de violaciones al derecho a la privacidad

Es indispensable que se lleve a cabo una investigación seria, independiente e imparcial de las instancias en las que se detecte o existan indicios de abuso en la utilización de herramientas de vigilancia.

Debe considerarse la posibilidad que el órgano de supervisión independiente tenga facultades de investigación y de acusación en causas penales para garantizar la autonomía e independencia de las investigaciones. Además, la sociedad debe ser informada de los avances y los resultados de este tipo de investigaciones.

5. Comentarios finales

La vigilancia sin controles democráticos como política de seguridad ha avanzado en México sin un debate público

informado y basado en evidencia. Las consecuencias que apenas se alcanzan a observar, gracias a filtraciones de información, son las de una proliferación de técnicas sofisticadas y masivas de vigilancia, como también el dispendio de cantidades enormes de recursos públicos, ejercidos con opacidad y siendo distraídos de otras medidas cuya eficacia para el combate a la inseguridad tiene mayor soporte empírico. Además, se ha demostrado la utilización de la vigilancia para fines ilegítimos, inclusive el espionaje político.

En un país donde la diferencia entre el Estado y la delincuencia organizada es, en ocasiones, borrosa o inexistente, es claro que la lógica de la necesidad del sacrificio de la privacidad para obtener seguridad no solamente es equivocada, sino que por el contrario, la seguridad, la libertad y la democracia se encuentran comprometidas ante el escenario de la vigilancia sin contrapesos.

No obstante lo anterior, persiste la oportunidad de revertir esta tendencia. En este artículo hemos ofrecido algunas vías para corregir el rumbo y comenzar, como sociedad, el respeto a nuestro derecho a la privacidad y con ello, las posibilidades reales de convivencia pacífica y democrática en México.

ANATEL y Consejo Ciudadano Ciudad de México. "Estudio e Investigación para el Desarrollo de Nuevas Medidas Tecnológicas que Permiten Inhibir y Combatir la Utilización de Equipos de Telecomunicaciones para la Comisión de Delitos", 2014. http://www.anatel.org.mx/Estudio_seguridad_2014.pdf (consultado el 5 de enero de 2016).

Angel, Arturo (2015a). "México, el principal cliente de una empresa que vende software para espiar", *Animal Político*, 7 de julio 2015, http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/ (consultado el 5 de enero de 2016).

Angel, Arturo (2015b). "Sedena negoció compra de software de Hacking Team en 2015 para espiar a 600 personas", *Animal Político*, 21 de julio 2015. http://www.animalpolitico.com/2015/07/sedena-negocio-compra-de-software-a-hacking-team-en-2015-para-espiar-a-600-personas/ (consultado el 5 de enero de 2016).

Aroche, Ernesto (2015a). "El Gobierno de Puebla utilizó el software de Hacking Team para espionaje político". *Animal Político,* 22 julio de 2015. http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/ (consultado el 5 de enero de 2016).

Aroche, Ernesto (2015b). "De manera sistemática gobierno de RMV manda infectar computadoras y móviles para espiar", *La Jornada de Oriente,* 13 de julio de 2015. http://www.lajornadadeoriente.com.mx/2015/07/13/de-manera-sistematica-gobierno-de-rmv-manda-infectar-computadoras-y-moviles-para-espiar/ (consultado el 5 de enero de 2016).

Devereaux, Ryan, Glenn Greenwald & Laura Poitras. "Data Pirates of the Caribbean: The NSA is recording every cell phone call in the Bahamas", *The Intercept,* 19 de mayo 2014. https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (consultado el 5 de enero de 2016).

Erasmus University Rotterdam (EUR). "Wie wat bewaart die heeft wat". Rotterdam: Faculteit der Rechtsgeleerdheid, 2005, http://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vi3anxk6vdy0 (consultado el 5 de enero de 2016).

Guerrero Gutiérrez, Eduardo. "Los hoyos negros de la estrategia contra el narco", *Nexos,* 1 de agosto de 2010. http://www.nexos.com.mx/?p=13844 (consultado el 6 de enero de 2016).

Heath, Brad. "U.S. secretly tracked billions of calls for decades", *USA Today,* 8 de abril de 2015. http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/ (consultado el 5 de enero de 2016).

La Rue, Frank. "Informe del Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas". 17 de abril de 2013, A/HRC/23/40. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (consultado el 5 de enero de 2016).

Lauv, Jason. "The NSA has set up shop at the US embassy in México", *Vice,* 24 de febrero de 2014. https://www.vice.com/read/the-nsa-has-set-up-shop-at-the-us-embassy-in-mexico (consultado el 5 de enero de 2016).

Planck, Max "Institute for Foreign and International Criminal Law. The Right of Discovery Concerning Telecommunication Traffic Data According to §§ 100g, 100h of the German Code of Criminal Procedure", marzo de 2008. http://dip21.bundestag.de/dip21/btd/16/084/1608434.pdf (consultado el 5 de enero de 2016).

Zuckerman, Johanna y Christine Murray. "Mexico ramps up surveillance to fight crime, but controls lax", *Reuters*, 12 de octubre 2015. http://www.reuters.com/article/2015/10/12/us-mexico-surveillance-idUSKCN0S61WY20151012 (consultado el 5 de enero de 2016).

Neutralidad de la red e internet en México: una perspectiva sociotécnica

Alejandro Pisanty y Erik Huesca

El concepto de neutralidad de la red ha sido objeto de intensos debates en años recientes, con consecuencias importantes para la regulación y el futuro del mercado y operación de internet en varios países. En México, el organismo regulador está a punto[1] de emitir reglas con base en este concepto.

Existen diversas definiciones de la neutralidad de la red, que tienen en común la no discriminación de comunicaciones en internet con base en origen, destino o contenido.

El concepto de la Coalición Dinámica sobre Neutralidad de la Red del Foro de Gobernanza de Internet es: el principio de acuerdo con el cual "el tráfico de internet será tratado sin discriminación, restricción o interferencia, independientemente del remitente, destinatario, tipo o contenido, de tal manera que la libertad de los usuarios de internet no se vea restringida por favorecer o desfavorecer de manera no razonable la transmisión de tipos específicos de tráfico".[2]

1 N. del E.: a enero de 2016 tal regulación todavía se encontraba pendiente.

2 Dynamic Coalition on Network Neutrality (DCNN), "Network Neutrality Policy Statement", Internet Governance Forum, 5 de agosto de 2015, http://review.intgovforum.org/igf-2015/dynamic-coalitions/

Para comprender mejor la idea, ubicar los debates y participar eficazmente en la toma de decisiones, es conveniente revisar las bases técnicas del diseño y operación de internet relevantes en la discusión.

El concepto de neutralidad, como se debate en la mayoría de los casos, es principalmente un problema de reestructuración de mercados, que a su vez, como actividad económica, tiene impacto sobre los derechos humanos. En la práctica, la neutralidad es inexistente a nivel técnico porque la tecnología de internet fue concebida para que las redes sean administradas. Los objetivos de la administración van desde la supervivencia misma de la red hasta la optimización de la experiencia de los usuarios, e incluyen respuestas a la congestión, a limitaciones de recursos, a políticas públicas y a acuerdos comerciales.

Sin embargo, eso no quiere decir que no existan ciertos principios técnicos que se deben respetar para promover el derecho a la libertad de expresión y el acceso a la información en internet. Por ello, preferimos hablar de "Internet Abierta" como lo refiere la Internet Society (ISOC, 2010 y 2015), organización global que promueve la normalización técnica, la difusión universal y la capacitación sobre internet, y constituye el amparo corporativo de la Internet Engineering Task Force (IETF) agrupando a los profesionales de internet interesados en la relación entre tecnología y sociedad.

---

input-document-on-network-neutrality/dynamic-coalition-on-network-neutrality-dcnn/ (consultado el 16 de diciembre de 2015). [Traducción de los autores]

El enfoque de "Internet Abierta" va más allá de la neutralidad misma y busca asegurar que el acceso a internet no esté impedido por factores como incompatibilidad técnica, administración no apegada a buenas prácticas y falta de capacidad para operarla. En el fondo, remite a una regla básica de cooperación en internet, un principio de igualdad en el que no deben existir sesgos o abusos de poder en la transmisión de datos ajenos. Los principios de Internet Abierta incluyen capacidad de elección para los usuarios, competencia, transparencia en las decisiones sobre la operación y administración de las redes, no discriminación arbitraria y capacidad de innovación. La administración de la red debe ser "razonable", término que, si bien está sujeto a interpretación, excluye la explotación contraria a la competencia y a los derechos de los usuarios.

1. Enfoque técnico

Es necesario explorar los orígenes de la tecnología de internet con la finalidad de contar con un marco de referencia claro para el análisis del concepto de neutralidad de red, enunciado hace poco más de una década por autores como Lawrence Lessig y Mark Lemley (2001), Tim Wu (2003) y Barbara van Schewick (2010). Estos se refieren al principio "de punta a punta" (o "end-to-end") utilizado en el diseño de la tecnología y los estándares de internet, con un giro interpretativo propio, pues preveían el posible abuso comercial de algunos proveedores para favorecer sus contenidos, los de sus clientes y sus aliados.

Conviene empezar a entender esta distinción a partir de la arquitectura y operación de internet, dada la complejidad

en la estructura de las redes que la conforman y la forma en que hoy opera, ya que la gestión de la red sin intervención de los operadores y de decisiones sobre el tráfico (y su posible priorización o incluso rechazo) es imposible. No se debe olvidar que el tráfico de internet es estocástico, con un grado muy alto de aleatoriedad y variaciones extremas que lo hacen fundamentalmente impredecible. La gestión de redes asume esta imprevisibilidad y la administra.

Coloquialmente, el principio "de punta a punta" se suele explicar con una analogía: un banco que envía un sobre cerrado con el estado de cuenta de uno de sus clientes y solo el cliente conoce el contenido, sin que la oficina postal o el cartero lo inspeccionen en su tránsito. Los únicos que saben qué saldo tiene la cuenta son el banco y el cliente, es decir, el emisor y receptor. Lo mismo debería suceder con los protocolos de internet. El contenido se ensambla y se controla únicamente en las orillas o extremos.

En la literatura técnica sobre la forma en que opera internet aparecen términos como "paquetes" y "capas", los cuales hacen referencia a una abstracción sobre cómo operan las redes.

Se dice que la comunicación de internet es por "paquetes" porque en lugar de establecer un enlace entre dos extremos que se dedica íntegramente a estos mientras se comunican, los "mensajes" se dividen en distintos pedazos en el extremo emisor para transmitirse por diversas rutas. Cuando llegan a su destino son reensamblados y se vuelven entendibles para las máquinas, y luego (algunos de ellos) también para las personas.

Por otro lado, las "capas" agrupan conjuntos de acciones específicas para ejecutar una tarea determinada, como por ejemplo "entender" sobre qué medio físico se está transmitiendo la comunicación, determinar cuál es la mejor trayectoria para que el contenido alcance su destino o establecer cómo se controla la comunicación entre el origen y el destino mismo. Lo que sucede en cada capa asume que las capas inferiores están operando y proveen ciertos productos para dichas operaciones, pero no intervienen en esa capa inferior. Por otra parte, cada capa provee ciertos insumos para las operaciones de las capas superiores, sin interferir en sus operaciones.

La arquitectura y las operaciones de internet se definen en documentos llamados *Request For Comments* o RFC (los "estándares" comunitarios que delinean la arquitectura, operación e interacción de internet) producidos en la IETF. El modelo de cuatro capas está descrito en los RFC 768, 791, 792 y 793.

La primera es la capa física, es decir, los aparatos tangibles donde se transmiten datos, que pueden ser alámbricos o inalámbricos; fibra óptica o satélite. La segunda es la capa lógica, que tiene que ver con la interface del equipo que recibe el paquete. Por ejemplo, si un mensaje se emite desde un teléfono móvil, este aparato tiene una identificación física o puerto único en el mundo. Para efectos del concepto de "Internet Abierta" y el debate sobre neutralidad de la red, las capas relevantes son la tercera y la cuarta, porque son las que determinan el direccionamiento y enrutamiento, y controlan las comunicaciones. En conjunto operan el principio

"de punta a punta" y es donde más controversias hay por la gestión de tráfico. A continuación, revisaremos con detalle lo que ocurre en las capas tercera y cuarta en relación con el propósito de este artículo.

1.1. Capa tres: de dónde vengo, a dónde voy y por dónde paso

La capa tres tiene tres funciones: el direccionamiento lógico, el enrutamiento y la verificación de si los equipos en los extremos de la comunicación están disponibles.

El protocolo característico de esta capa es el protocolo IP (*Internetworking Protocol*), un conjunto de instrucciones entre sistemas para interconectar redes diversas. Cada equipo en la red es identificado por una dirección numérica llamada dirección IP; en IPv4,[3] estas direcciones se forman por triadas de números de hasta tres dígitos menores que 256, como por ejemplo 132.248.10.1.

El enrutamiento es la decisión sobre qué trayectoria tomar para evitar el congestionamiento de los enlaces que forman una comunicación. Al crecer la red y hacerse compleja en los años 90, la IETF propone innovaciones que permiten "etiquetar" el tráfico para poder diferenciarlo y darle distintas prioridades de transmisión sobre la red. Desde aquí, la red no es neutral ante el tráfico, pues trata de diferenciarlo: cada aplicación (voz, audio, video o datos) es sensible a los retrasos y congestionamientos en la red de manera distinta.

3 N. del E.: IPv4 es la cuarta versión del protocolo IP, definida en el RFC 791, que ha identificado direcciones de la red durante su expansión de las últimas décadas.

A partir de 1996, estos "servicios diferenciados" evolucionaron con la integración de voz, datos y video que existían en otras redes de telecomunicaciones separadas. Esto termina en la creación de protocolos para etiquetar y manipular cada uno de los paquetes transmitidos en la red y diferenciarlos por origen, destino, tipo de contenido y tipo de cliente: los *Multiprotocol Label Switching* (MPLS). Con ello, se asignan prioridades de transmisión para asegurar la calidad de servicio y se permite la unificación de distintos tipos de datos. Aquí, de nuevo, la red no es neutral ante el tráfico y la gestión es cada vez más compleja.

Un ejemplo común consiste en adaptar la operación de la red por horarios, de modo que el tráfico de correo electrónico y mensajería se favorezca durante horas laborables y el de video en horarios de descanso. Otro tanto se aplica a bajar la prioridad del tráfico de video en situaciones de congestión, como eventos masivos o desastres.

Es muy importante dejar claro que hablar de "Internet Abierta" no equivale a hablar de internet sin fronteras. Por ejemplo, para optimizar el enrutamiento, se vio la necesidad de crear números de identificación autónomos (*Autonomous System,* AS) para agrupar un gran conjunto de direcciones y simplificar el paso de comunicaciones a través de la red. Lo que hace esto es crear una frontera, por ejemplo, entre distintos tipos de empresas de telecomunicaciones y sus clientes. Es decir, una empresa de telecomunicaciones "X" tiene su número autónomo AS y con ese entrega el tráfico de sus clientes con la empresa "Y", que tiene otro número

autónomo diferente. Si bien las fronteras no están ligadas a referencias geográficas, sí lo están a los principios de administración de cada una de las redes.

Las fronteras se relacionan con la capa tres, pues el dueño de cada red tiene libertad para decidir las políticas con las que las administra su tráfico, siempre y cuando se preserve el principio de cooperación en internet: un principio de igualdad en el que no deben existir sesgos o abusos de poder en la transmisión de tráficos ajenos.

1.2. Capa cuatro: donde se controlan las comunicaciones y se tienen aplicaciones propias de internet

En esta capa se encuentran dos protocolos que controlan la comunicación y el conjunto de aplicaciones de internet, que conectan con "puertos bien conocidos" como web que es el puerto 80, la transferencia de archivos que es el puerto 21 o el correo electrónico que es el puerto 25.

Aplicaciones como Apple Music o Netflix usan un conjunto de estos puertos y operan sobre la red; por ello son conocidas como OTT (*Over The Top*)[4] o como OSP (*Online Service Providers*). Por esta razón, no trataremos estos últimos den-

4 La denominación *Over The Top* indica servicios o aplicaciones que se definen arriba de las capas de la arquitectura de red, y se originó en la industria de telecomunicaciones, tanto la de TV por cable como la que está conformada por compañías telefónicas y proveedores de acceso a internet (que a veces son las mismas compañías). Hemos decidido utilizar esta terminología a pesar de estar sujeta a una controversia en la comunidad técnica de internet.

tro de la estructura de la capa cuatro. Sin embargo, son estas aplicaciones de cómputo las que hoy están provocando las mayores controversias por el tráfico que generan en las redes de los distintos operadores.

Los dos protocolos para controlar la comunicación "punta a punta" en la capa cuatro son *User Datagram Protoc*ol (UDP) y *Transmission Control Protocol* (TCP). La diferencia fundamental entre ellos, es que UDP deja a la aplicación de internet o de cómputo ensamblar la comunicación. El *streaming* de video usa UDP y por eso los datos a veces no llegan todos completos y podemos ver cuadros que se congelan o se saltan, sin perder el conjunto del video. Por otro lado, TCP controla la comunicación por cada datagrama o paquete emitido, su secuencia y la pérdida de paquetes, hasta lograr el ensamblado de la comunicación. Es decir, la comunicación no se lee a menos que esté completa.

Como se puede apreciar, la tecnología de internet ha tenido desde un principio los métodos necesarios para administrar y manipular tráfico, sobre todo en redes multiprotocolo. Por ello, desde su origen -tanto en las computadoras, como en los enrutadores- existió la capacidad de manipular y diferenciar servicios de acuerdo al tipo de puerto bien conocido en capa cuatro y de direcciones o protocolo de enrutamiento en capa tres.

La gestión técnica de la red está orientada a mantener la integridad de las comunicaciones, evitar problemas de congestión y asegurar continuidad a las transmisiones. La IETF

tiene grupos de trabajo y documentos de buenas prácticas sobre este aspecto, además de los estándares para su construcción e implementación.[5]

Los problemas que se pueden identificar como de neutralidad de la red que se dan en las capas tres y cuatro son los siguientes:

- Filtrado, bloqueo, retraso y estrangulamiento. Diversos equipos y software permiten limitar el paso de paquetes dependiendo de origen, destino, protocolo o puerto hacia sus destinatarios. Pueden hacerlo de manera temporal o permanente y absoluta o relativa; es decir, pueden bloquear el paso de los paquetes o limitar la velocidad a la que son entregados. Este estrangulamiento puede producir en el destinatario la impresión de una deficiencia de servicio del remitente, al punto de llevarlo a interrumpir su relación comercial con el mismo. La introducción de retraso o *jitter* (variación en el retraso) puede hacer que algunas aplicaciones funcionen muy deficientemente, especialmente las de video y las comunicaciones bidireccionales.

- Inspección de paquetes o *deep packet inspection*. El tráfico en las redes pasa por numerosas fronteras entre su origen y destino. En cada frontera, si se desconoce una dirección, hay dos posibilidades: rechazar el tráfico o enviarlo sin procesar a otro dominio administrativo (es decir, a otro *Autonomous System*). Existe un fuerte incentivo para que los operadores optimicen su negocio,

5 Se pueden consultar en su sitio, https://www.ietf.org/

aplicando la inspección de los paquetes, *deep packet inspection* o DPI. Por ejemplo, se inspeccionan paquetes para conocer si usan protocolos como *peer-to-peer* –usados para el intercambio de música, como lo era Napster, o la VOZ-IP, como Skype– que generalmente son restringidos porque congestionan mucho la red, que siempre tendrá recursos limitados.

Estrictamente hablando, la DPI es una violación de la "Internet Abierta" porque al inspeccionar el contenido que guardan los paquetes y comunicaciones, rompen la cooperación igualitaria, violando el principio de "de punta a punta" y el de "independencia entre capas". Primero porque, como vimos, el principio de "punta a punta" establece que el emisor y el receptor son los únicos que deben conocer el contenido de los mensajes: si se inspeccionan los paquetes, esto implica que los intermediarios conocen el contenido de los mensajes. Segundo, porque para "abrir" un paquete, se deben intervenir las capas tres y cuatro, para poder llegar al contenido. Esto además atenta contra el derecho a la privacidad de las comunicaciones de los ciudadanos en las redes.

- SOBRESUSCRIPCIÓN DE CAPACIDAD. Los operadores de telecomunicaciones normalmente no invierten al ritmo de la demanda de anchura de banda requerida para las aplicaciones como Netflix, iTunes o Google, entre otras. Al no invertir, utilizan estrategias para simular servicios que hoy no son capaces de entregar. Para el caso de redes alambradas –fibra óptica o cobre con DSL, incluyendo

WiFi– la práctica usada es la sobresuscripción o sobreventa más allá de las capacidades de la red misma.

En las redes inalámbricas de telefonía móvil o satelitales, el problema se agrava porque desde el punto de vista técnico, existe poca disponibilidad del ancho de banda.

Hay sobresuscripción y además incremento de prácticas como el *zero-rating*, que implica la posible colusión de los operadores de telecomunicaciones con los operadores de servicios OTT. Estos últimos suelen ser los mismos mencionados en las aplicaciones de cómputo: compañías como Netflix, Google, Facebook, etcétera. El *zero-rating* implica no cobrar a los suscriptores de servicios de telecomunicaciones por el uso de alguna de estas últimas aplicaciones o servicios.

- EL USO DE EQUIPOS *LEGACY*. Se llama *legacy* ("herencia") al equipo y software instalado con mucha anterioridad, generalmente sin documentación y cuyos administradores originales han dejado la organización. Hoy en día todavía operan muchos equipos de clientes y operadores que utilizan *software* de hace más de 10 años, incapaces de interpretar protocolos nuevos como el IPv6. El problema es que no existe la capacidad para hacer direccionamientos más precisos. La continuidad del uso de estos equipos se produce porque a lo largo de décadas el protocolo TCP/IP ha estado en operación en su versión 4 o IPv4 sin cambios radicales. Pero esos equipos son incapaces de incorporar de forma eficiente las mejoras de

protocolos como ICMP, BGP, TCP y UDP ni de operar con IPv6, la sexta versión del protocolo IP. Este fenómeno es parte de la deuda técnica en la que han incurrido la mayoría de operadores y clientes.

- El uso de aplicaciones OTT. Al centro de la discusión sobre mercado y neutralidad están los proveedores de servicios que no forman parte de internet, pero usan algunas de sus aplicaciones para comunicarse, conocidos como OTT. Estrictamente hablando, estas aplicaciones existen fuera del modelo original de cuatro capas, pues solo usan un puerto bien conocido y el protocolo IP. Esta operación es paradójica, pues permite a operadores vender capacidad de acceso a la red y, al mismo tiempo, complica la operación de la misma.

- Uso indiscriminado de comunicaciones a través de mecanismos como NAT (*network address translation*) o *firewalls*. Este es el primer momento donde una red es manipulada en su tráfico. La primera tiene la finalidad de usar el mapeo de una dirección enrutable a muchas ofuscadas. El segundo dispositivo se usa para evitar visitas inoportunas a la red propia.

La gestión de tráfico en las redes que se interconectan en internet varía de acuerdo a la demanda y a las capacidades de los operadores.

Desde el punto de vista técnico, la neutralidad de la red que se demanda en la actualidad es en gran medida una ficción, pues la neutralidad respecto a orígenes, destinos y contenidos, sin

bloqueos ni priorizaciones, no es factible en la práctica.

Las políticas de administración son diferentes en cada dominio administrativo, lo cual es una libertad fundamental contra la que no debemos atentar. Cada operador es libre de administrar su red, con las reglas y formas que están a su alcance económico, técnico y administrativo. Las redes que forman internet son diferentes en anchura de banda, en software, en equipamiento y, como ya dijimos, en reglas de administración. Esta magna cooperación en libertad es la raíz de la explosiva expansión de internet.

La mayor parte de esta complejidad permanece fuera de la vista del usuario final, aunque es vital para los operadores y grandes usuarios. Necesitamos ahora una definición, más que de neutralidad de red, de "Internet Abierta" adecuada y susceptible de ser puesta en operación y adaptable a circunstancias cambiantes en el futuro.

2. Enfoques regulatorios

Los usuarios de internet tienen mayor capacidad de intervención en ámbitos como el regulatorio, el político, los derechos de los usuarios y ciudadanos, que en el establecimiento de estándares técnicos o en la operación de grandes redes de telecomunicaciones.

Los abordajes al problema de apertura de internet –más que neutralidad de la red- varían entre países. Una forma de clasificarlos es mediante el enfoque regulatorio adoptado, que corresponde también a una instancia de regulación. Reconocemos los siguientes enfoques regulatorios:

- Enfoque regulatorio desde lo técnico. La situación técnica de internet, apegada a sus estándares y las condiciones de heterogeneidad y complejidad en el transporte y acceso a la red, nos lleva a afirmar que la neutralidad debe estar sujeta a vigilancia y, en caso de violaciones, reclamación. Debe permitir que cualquier ciudadano experto o auxiliado por expertos técnicos reclame las violaciones a la neutralidad directamente a su proveedor. Este principio recoge la descripción de neutralidad de la red de las secciones iniciales.

  Las transformaciones radicales que internet produce en la sociedad se basan en que los usuarios pueden ser también productores de contenidos y servicios, no solo consumidores. Mantener la neutralidad de la red al máximo permitido por esta interpretación técnica es indispensable para la innovación en las aplicaciones.

  Si bien en México la producción de innovaciones en la red es muy limitada (menos de .01% de las contribuciones técnicas a la IETF provienen de Latinoamérica), el ambiente de innovación en las aplicaciones está muy activo y enfrenta barreras de entrada mucho menores. La neutralidad de la red sirve especialmente a este sector. Esta visión específica coincide con la del regulador estadounidense de telecomunicaciones, la Federal Communications Commision (FCC) y privilegia la innovación "en la orilla", en las aplicaciones, mientras que la europea da mayor peso a la red misma.

- Enfoque centrado en el consumidor. Se puede construir una perspectiva de la neutralidad de la red a partir de los derechos de los consumidores. Para que sea efectiva, los contratos de los consumidores con sus proveedores –generalmente contratos de adhesión que el cliente no tiene opción de modificar– deben especificar el alcance de los servicios de acceso a internet en forma muy amplia. Todavía mejor si los contratos incluyen la neutralidad de la red de manera explícita o por referencia a un mandato de ley existente. En estos casos, los usuarios reclamarán las posibles violaciones a la neutralidad ante las autoridades de protección de los consumidores, así como en referencia a violaciones a los derechos de los usuarios establecidos en la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) de México.

- Enfoque centrado en los derechos del ciudadano: En este enfoque el eje está en los derechos políticos y civiles, e incluso los económicos más allá de los de los consumidores, como causal de reclamación por neutralidad. Entre los derechos de rango supralegal considerados en este enfoque están la libertad de expresión, el derecho a la educación, el derecho a la información y la libertad de asociación. Se enfatiza el posible papel de violaciones a la neutralidad de la red sobre dichos derechos, por ejemplo, por medio de filtrado, bloqueo o entorpecimiento del acceso a determinados contenidos y potencialmente también el acceso a algunos puertos portadores de protocolos diversos, como los de mensajería y telefonía sobre IP y los usados para el cifrado de la información.

Es importante señalar que los artículos 122, 145, 146, 189, 190 al 197 y 216 de la LFTR, transforman un derecho constitucional en una concepción netamente mercantil de usuarios de servicios de telecomunicaciones. El enfoque centrado en derechos fundamentales es el más apropiado para los ciudadanos y las organizaciones dedicadas a la promoción y defensa de los derechos por su claridad; a cambio, presenta la dificultad de probar las violaciones a esos derechos y, sobre todo, su base en prácticas contrarias a la neutralidad de la red.

- Enfoque basado en la competencia comercial. En este enfoque se caracterizan las violaciones a la neutralidad de la red como intervenciones contra la libre competencia, tales como competencia desleal, acciones anticompetitivas, colusión y otras. Las violaciones en este marco deben ser reclamadas ante las autoridades vigilantes de competencia económica.

  En el marco legal mexicano sería improbable que los consumidores o ciudadanos individuales lograran impulsar un caso de esta naturaleza mediante acciones colectivas. La investigación podría provenir de la iniciativa de la propia autoridad.

  Cabe recordar que el derecho de competencia usa la regulación *ex post* aparte de reglas generales, por lo que hay que esperar a que un actor del mercado haya ejercido indebidamente su poder dominante o preponderante para reclamarlo.

Como marco más amplio del enfoque de competencia, el enfoque centrado en el mercado confía en que, en un mercado maduro, la "mano invisible" se encargará que al menos un proveedor preste servicios de internet en los que garantice la neutralidad. Este punto es optimista pues excluye posibilidades de colusión y "cartelización" sutiles, o que la prestación del servicio de acceso irrestricto a internet solo sea ofrecida a costos fuera del alcance de usuarios y ciudadanos. Es el enfoque adoptado como principio mayor en Europa. Diversas escuelas de pensamiento tienen puntos de vista diferentes sobre la necesidad de intervención del Estado en esta regulación y el nivel de la misma.

- Regulación de telecomunicaciones. La regulación de telecomunicaciones se orienta actualmente a que la asignación de recursos técnicos y concesiones de operación de servicios públicos operen en función del servicio público y sin que la asignación de recursos cree artificialmente condiciones contrarias a la competencia. Generalmente, esto se aplica a los recursos escasos y de utilización excluyente que son propiedad pública, como el espectro radioeléctrico y las concesiones para la prestación de servicios como telefonía y radiodifusión. En general, en México ser concesionario tiene una connotación de propiedad sobre el recurso concesionado, situación que dificulta la vigilancia del cumplimiento de los títulos de concesión.

  En este esquema, el acceso a internet ha sido considerado hasta muy recientemente un servicio de informa-

ción o de valor agregado no regulado. En la actual LFTR mexicana, el concepto de servicio de valor agregado desapareció y todos los proveedores, incluso los académicos, están sujetos a concesión. De manera similar, en Estados Unidos el enfoque de la FCC representa también un paso hacia la consideración del acceso a internet como servicio sujeto a regulación de telecomunicaciones. Esta decisión consiste en extender a internet la aplicación de las normas de operadores concesionados, pero con *forbearance* (abstención); y aceptar los servicios especializados solo previo análisis caso por caso.

3. Otros aspectos de la neutralidad de la red

Hay otras importantes formas de caracterizar las controversias alrededor de la neutralidad de la red, parcialmente superpuestas a los enfoques regulatorios ya descritos.

3.1. Controversias comerciales de la neutralidad de la red

La principal controversia comercial en la red se produce entre operadores de red y proveedores de servicios que utilizan la red. Para simplificar, se suele hablar de operadores (incluyendo operadores de redes, compañías telefónicas e ISP, especialmente los del "tier 1" que son grandes redes troncales de alcance internacional y sus correlatos nacionales) y de OTT, compañías que proveen video, conversaciones sincrónicas de voz y video, mecanismos de creación de contenido para los usuarios, búsqueda y muchos otros servicios a través de internet. La controversia comercial se plantea en términos de quién paga qué servicios y a quién, y en qué punto de la red; cuáles son los centros de costo y los de utilidad, así como las

inversiones de capital y operativas, los rendimientos de la inversión y sus tiempos de recuperación para los distintos participantes comerciales.

La inversión de las compañías telefónicas está altamente regulada y tiene un gran componente de capital de lenta recuperación. Comparativamente, los proveedores de servicios que usan esta infraestructura y en particular los OTT tienen menor costo regulatorio, menores –aunque no insignificantes– inversiones de capital, mayor liquidez y tiempos de recuperación más cortos. Sus riesgos a corto plazo son sumamente altos, ya que sus mercados están expuestos a disrupciones radicales; algunas empresas en este segmento pueden ser borradas de la faz de la Tierra en cuestión de meses (como ocurrió con AltaVista y Hi5).

Algunos casos especialmente difíciles de tratar se presentan cuando los servicios de los OTT son utilizados en países en los cuales el proveedor no tiene presencia legal alguna y las compras de sus servicios se realizan mediante transacciones privadas internacionales por parte de los consumidores.[6]

6 Los modelos de negocio de los distintos actores varían enormemente. Muchos OTT obtienen sus ingresos y utilidades a partir de publicidad y venta o explotación analítica de la información de sus usuarios. Algunos no tienen activos físicos en la base de su operación y actúan solamente como corredores: por ejemplo, la *sharing economy* de transportes en automóvil (Uber) o de alojamiento (Airbnb). Dependiendo del modelo de negocio, algunos grandes OTT han creado sus redes. Su poder de compra y capacidad de inversión los pone ante los operadores de redes sobre una base de poder de negociación ya que, por otra parte, los operadores necesitan dar paso a su tráfico para conservar a sus clientes.

La complejidad de las interconexiones entre redes y los pagos, compensaciones, prestaciones y contraprestaciones de este mercado es enorme y no permite una determinación fácil de los cargos que cubrirán los costos. En esta afirmación se contiene también el hecho que el tráfico IP incluye una fracción duplicada cuando se requieren reenvíos de paquetes por congestión o fallas. Dicha fracción es medida y cobrada a los clientes.

Como consecuencia de lo descrito, algunos operadores consideran injusta la asimetría de los modelos de negocios en internet. Expresan que ellos hacen un negocio de largo plazo, altamente competido, dependiente de inversiones de lenta recuperación y bajo retorno, sometido a regulaciones que a su vez implican costos. En cambio, los OTT no dependen de hacer inversiones comparables en activos físicos, ni pasar por procesos regulatorios. En este punto, los operadores reclaman una parte del negocio de los OTT para sí. En países en los que el *common carriage* es una fuerte tradición, como Estados Unidos, estos argumentos son especialmente poco bienvenidos.

La teoría en la que se basa la regulación emergente de neutralidad de la red en Estados Unidos es la del "círculo virtuoso", en el que la aparición y aceptación de nuevos servicios en las capas altas y OTT produce demanda sobre los operadores de la red, y esta demanda produce pagos a los operadores que les permiten seguir haciendo inversiones en capacidad.

Otra tendencia en curso es la integración vertical –OTT que hacen redes y operadores que ofrecen OTT propios– que au-

menta las oportunidades e incentivos de colusión contraria a la libre competencia y a los intereses de los consumidores, ya que en estos casos el operador de red y el proveedor de servicio son el mismo.

3.2. Estructura del mercado: redes y servicios o mercados de dos caras

La economía de los mercados de dos caras está en el centro de las controversias sobre neutralidad de la red. Como hemos dicho, muchos puntos contenciosos se centran en cómo y dónde cada empresa obtiene ingresos y utilidades, y los intercambios entre ellas. Las controversias en Estados Unidos entre Google y Verizon y entre Netflix y Comcast son claros ejemplos.

Los mercados a los que nos hemos estado refiriendo tienen una complejidad: muchos de ellos son mercados de dos caras. Ejemplos arquetípicos de mercados de dos caras son los diarios y revistas, y la televisión restringida, que al mismo tiempo ofrecen contenidos y programas a los consumidores, y venden publicidad a los grandes anunciantes. El precio de la publicidad depende del número de espectadores; el número de espectadores depende del atractivo de la programación.

Las empresas emblemáticas como Netflix, Facebook, Google y Microsoft funcionan *prima facie* como proveedores de programación de video, servicios de búsqueda en internet y de creación, almacenamiento y distribución de contenidos. Algunas compañías proporcionan sus servicios sin cargo directo a los usuarios individuales; en estos casos, el flujo de

ingresos está determinado por la venta de anuncios comerciales y la explotación comercial de los perfiles altamente complejos y distintivos que se pueden formar de los usuarios mediante análisis estadísticos, involucrando además a terceros como los *data brokers*. Esta situación se suele abreviar diciendo que estas compañías "venden" a sus usuarios (es decir, información sobre los mismos) o con la frase "si el servicio es gratuito, tú eres la mercancía".

El operador también cumple dos funciones que definen un mercado de dos caras: se describe así al operador de red como una "plataforma" a la que el usuario también paga para el acceso.

Las redes evolucionan dinámicamente; el crecimiento del número de usuarios individuales va aproximadamente a la par de los servicios de los OTT y OSP; y las inversiones de ISP, Tier 1, OTT y OSP guardan cierta proporcionalidad. Difieren, en cambio, en tiempos de retorno, intensidad de capital, carga regulatoria, carga fiscal y la forma y sitio en el que se recuperan. Desde este punto de vista, la controversia sobre neutralidad de la red es la controversia sobre la distribución de los costos, los ingresos y las utilidades entre los distintos actores del mercado.

3.3. Enfoques regulatorios estadounidense y europeo: el rol del Estado

La diferencia entre los enfoques estadounidense y europeo ha sido estudiada con particular detenimiento, claridad y continuidad por J. Scott Marcus (2014). Es importante com-

prenderla porque ambos enfoques son ampliamente citados, se refieren a algunos de los mercados regulados de forma transparente más cuantiosos del planeta (dejando de lado mercados imperfectos aunque cuantiosos como el de China) y son el espacio en el que realmente le importa la neutralidad de la red a los grandes actores globales. De allí que lo que estos traigan a la mesa en un país como México esté filtrado por la suma de los enfoques internacionales y las circunstancias nacionales.

En Estados Unidos, la neutralidad de la red, antes que una discusión como un derecho, fue objeto de un debate intenso en el marco regulatorio de las telecomunicaciones y en el de las relaciones comerciales entre OTT como Netflix y Google, y operadores como Comcast y Verizon, respectivamente.

Los mercados de acceso local a internet en Estados Unidos presentan poca diversidad de oferta, mientras que en Europa esta es competitiva. Los OTT que más tráfico generan a nivel mundial, como los mencionados Netflix, Google, Facebook y Microsoft, son estadounidenses y no hay pronósticos de ser substituidos próximamente, lo cual afirma la importancia de analizar sus casos. La intervención de la FCC puede tener impactos directos e indirectos inesperados y perniciosos, que no es posible prever con certeza actualmente.

En Europa, la visión regulatoria de la neutralidad de la red busca ante todo evitar situaciones anticompetitivas entre operadores de red, así como garantizar la rentabilidad de sus inversiones, y solo en segundo orden regular la relación con

los OTT (Sorensen, 2015). En cambio, en Estados Unidos el debate regulatorio busca limitar el poder de los operadores sobre la provisión de servicios de internet.

Por ello, en Europa la mayoría de los reguladores –y su agrupamiento en BEREC (Body of European Regulators of Electronic Communications)– mantienen una posición de vigilancia, mientras en Estados Unidos la FCC trata de intervenir en el mercado de provisión de internet (por separado del de telecomunicaciones).

En Europa, por otra parte, las empresas y las asociaciones de industria se expresan con mucha mayor frecuencia e intensidad oponiendo las obligaciones de neutralidad de la red (actuales o potenciales) a la preservación de las condiciones para la inversión. El argumento no ha sido presentado de forma cuantitativa.

Podemos prever que en Latinoamérica la regulación de neutralidad de la red será adaptada de uno de los dos enfoques principales, con una combinación adicional de componentes del otro. Los operadores y las empresas globales no analizarán solamente mercados aislados, sino al menos los continentales.

Algunos de los efectos que pueden resultar inesperados provendrán de la inserción del Estado en espacios de internet que hasta ahora han sido libres de intervención estatal, como la necesidad de vigilar el contenido de las comunicaciones para evitar violaciones a la neutralidad de la red, vigilancia que puede ser extendida para fines no regulatorios.

Dicha intervención significa un paso importante, ya que hasta ahora la regulación de los servicios de telecomunicaciones se ha limitado a la infraestructura, prácticamente confinada a la capa física, mientras que los servicios de internet se han considerado como de información, usando las telecomunicaciones pero sin necesariamente ser regulados como concesionarios de este servicio público. Aún está por resolverse si se abrirán todas las redes a la competencia (*open access*) o si se limitará la competencia directa (*Open Internet* en la versión de la FCC)[7].

3.4. El locus de la controversia: última milla al usuario final, interconexión, transporte

En lo que hemos descrito hasta ahora conviene destacar que los pagos, cobros, transferencias e inversiones que se tratan en las controversias sobre neutralidad de la red varían entre países e incluso entre casos particulares, en función de si la interpretación de neutralidad como cobro indebidamente discriminatorio tiene efectos en la "última milla" al usuario. Si no es este el caso, el debate puede referirse a otros puntos descritos en el presente trabajo.

3.5. La importancia de la neutralidad en la innovación

La neutralidad de la red puede impulsar o inhibir la innovación, de acuerdo con diferentes autores. Según algunos especialistas, la mayoría de las innovaciones alcanzadas utilizando internet han sido posibles gracias a la ausencia de

7 Conforme a las denominadas "Open Internet Rules" de la FCC, vigentes desde junio de 2015.

interferencias y tratos discriminatorios en la red. Grandes empresas como PayPal, Google, Facebook, Skype y muchas otras empezaron con innovaciones radicales, cuya supervivencia no hubiera estado garantizada en un entorno más fuertemente regulado.

El fundamento económico de este enfoque reside en la idea de que permitir la innovación lleva a la creación de nuevos servicios y estos, a su vez, producen nuevo tráfico que es rentable para los operadores de redes. Layton (2014) ha puesto a prueba este principio con estudios empíricos que hasta ahora no lo ratifican, aunque no hay todavía evidencia suficiente para descartarlo.

Según otros análisis, la neutralidad de la red puede inhibir la prestación de servicios necesarios como los de alta velocidad, baja latencia y otras características de las redes. Algunos de estos servicios no pueden plantearse sobre la premisa de "mejor esfuerzo" de internet, especialmente si los operadores pueden utilizar técnicas de gestión de tráfico para cumplir con SLA (*Service Level Agreements*, acuerdos de nivel de servicio que proveen algunas garantías de acotar valores de variables como latencia y velocidad de transmisión), pero, por otra parte, no pueden plantearse en todos los sitios geográficos sobre enlaces dedicados y de características de transmisión predeterminadas, ya que pueden no estar disponibles o alcanzar costos prohibitivos.

Este argumento es esgrimido por las compañías telefónicas y grandes operadores de redes europeas agrupadas en ETNO

(European Telecommunications Network Operators), cuya voz cantante en la actualidad llevan la propia ETNO, Telecom Italia y Telefónica, tanto desde su matriz en España como a través de sus representaciones en otros países. La innovación que favorecen se refiere con frecuencia a modelos comerciales y no a nuevos servicios en capas superiores o a nuevas aplicaciones.

También está en juego aquí la posible innovación en tecnologías para crear, administrar y monetizar escasez dentro de la red, como puede ser la provisión de anchura de banda, límites a las latencias y conexión selectiva a servicios y OTT. Este punto es axial para la idea misma de neutralidad de la red: innovación en la orilla, sobre una red que no escoge ganadores, o innovación determinada en el corazón de la red, que puede excluir a innovadores en la orilla por el costo de acceso requerido para aplicaciones especializadas.

También debemos reconocer argumentos desde la comunidad técnica de internet en contra de la regulación de la neutralidad de la red y que invocan la innovación. Para ellos, la regulación excesiva es por sí misma un inhibidor de la innovación, mientras que las fuerzas del mercado son consideradas suficientes para seleccionar a las innovaciones que deben ser duraderas y descartar a las que no lo serán.

3.6. Modelos de regulación: *soft law* versus *hard law*

Se puede distinguir entre esquemas auto o corregulatorios y sistemas basados en legislación prescriptiva explícita. Los enfoques de *soft law* incluyen mecanismos como la auto y

corregulación de los operadores de red, la negociación de acuerdos comerciales entre estos y los OTT, y la observación y diálogo con las autoridades y los consumidores. En mayor o menor medida pueden ser considerados modelos de participación multisectorial.

Estos enfoques han sido exitosos en los países escandinavos. Tienen como ventajas la prevención de sorpresas, la adaptabilidad a condiciones cambiantes y la escucha de múltiples sectores. Su principal desventaja está en el riesgo que algún actor abandone el esquema y cree un servicio o cobro que viole las reglas o decida resolver una controversia a través de litigios. En este caso, ese actor tiene fácil acceso a argumentar aplicaciones retroactivas de la ley y ausencia del estado de derecho.

Los enfoques de *hard law* se basan en la emisión de leyes y regulaciones por las autoridades pertinentes. Las leyes pueden ser insuficientes para abarcar los casos, estar atrasadas respecto a la realidad operacional, presentar oportunidades de simulación o de obstaculización mediante litigios o requerir sucesivas reglamentaciones de grano fino, susceptibles de captura por alguno de los actores. Es el caso de algunos países como México y del Marco Civil de Internet en Brasil.

Este enfoque tiene como ventaja la certeza jurídica en países donde rige el derecho positivo, y como desventaja la rigidez, el desfase respecto a la realidad, la falta de oportunidades explícitas de intervención de sectores afectados y el riesgo de captura legislativa o regulatoria por los actores profesionales de mayor poder económico.

4. Paradojas de la neutralidad

Es necesario subrayar una posible paradoja: al clamar por neutralidad de la red, las partes que lo hacen pueden estar invocando una intervención del Estado en varios planos en que los mismos actores han preferido su ausencia. Para regular y vigilar el cumplimiento de la neutralidad de la red, diversos órganos del Estado, en los tres poderes, pueden estar regulando más que el sentido más escueto de la neutralidad de la red. Para juzgar sobre una acusación de trato discriminatorio, es concebible que el Poder Legislativo haya tenido previamente que establecer la ley respectiva; que el Ejecutivo o un regulador (de libre competencia, de telecomunicaciones o de derechos del consumidor) tenga que establecer una inspección permanente del tráfico y sus características; y que el Judicial se vea obligado a inspeccionar el contenido del tráfico, no solo los metadatos, para juzgar en un litigio en la materia. Para saber si se discrimina en función del contenido es necesario inspeccionarlo.

Este argumento es esgrimido con frecuencia desde posiciones liberales de mercado cercanas a las empresas, pero no puede ser ignorado por la sociedad civil. Los efectos de este tipo de regulación deben ser objeto de un cuidadoso análisis de riesgos.

La legislación establecida para la neutralidad de la red proviene generalmente de alguna combinación de las perspectivas ya descritas. En los casos de Holanda, Bélgica y Chile, la ley fue establecida en respuesta a bloqueos o filtrados selectivos lesivos a los intereses de los consumidores realizados

por los operadores. En Europa, los reguladores han partido de un principio de parsimonia, pero observan atentamente la evolución de la conducta de los operadores, como en el caso en Inglaterra, Francia y el colectivo de los reguladores europeos (BEREC).

En octubre de 2015, el Parlamento Europeo aprobó normas generales para el continente en materia de neutralidad de la red.[8] En ellas se enfatiza el principio de no discriminación de tráfico, se autoriza la gestión razonable de las redes, se permite a los operadores crear canales para servicios especializados y se deja pendiente una consulta para términos detallados de la reglamentación y la regulación a nivel nacional en los países del continente.

Para los defensores de derechos es imprescindible observar esta legislación atentamente, pues tendrá una fuerte influencia en México y en América Latina en general. Se puede pronosticar que formará parte de los argumentos de los operadores en pro de la reglamentación que favorecerán, pues ya ha sido el caso en la propia Europa. Los servicios especializados, la laxitud de la norma, el enfoque en preservar la innovación en la red (en lugar de en la orilla) y el énfasis en preservar las condiciones para la inversión de los operadores son las "huellas digitales" de este enfoque.

La revista *The Economist* (2015), hace un resumen particu-

8 N. del E.: Resolución legislativa del Parlamento Europeo, de 27 de octubre de 2015, sobre el denominado "Mercado único europeo de las comunicaciones electrónicas".

larmente compacto de lo anterior y explica las diferencias entre los enfoques norteamericano y europeo inequívocamente, tomando como causa la diferencia en pesos relativos de las capacidades de influencia y el cabildeo de las empresas operadoras de redes (mayor en Europa) y de las proveedoras de innovación sobre las redes (mayor en Estados Unidos).

La legislación chilena ha sido interpretada, además, como contraria al *zero-rating*, que ha quedado prohibido en ese país con base en ella. En los Países Bajos, la prohibición del *zero-rating* es explícita y es posible que deba ser sobreseída por las normas europeas derivadas del Mercado Único Digital. En otras jurisdicciones esta materia está pendiente de resolución.

Durante los procesos previos a la WCIT (World Conference on International Telecommunications, orientada a revisar los Reglamentos de Telecomunicaciones) de la UIT en 2012, la ETNO y algunas de sus empresas miembros, realizaron una intensa campaña contraria al reconocimiento explícito de la neutralidad de la red, argumentando que esta norma aumentaría la carga regulatoria sobre los operadores hasta volver incosteable su operación y nugatoria la recuperación de sus inversiones. Este argumento se puede reconocer en la legislación mexicana sobre neutralidad de la red, en la cláusula final del artículo correspondiente de la LFTR, que indica la necesidad de mantener la inversión en redes.

El Foro sobre Gobernanza de Internet (IGF) se ha ocupado de la neutralidad de la red en diversas sesiones a lo largo de los años. A partir de 2013, además de las sesiones generales,

existe la Coalición Dinámica sobre Neutralidad de la Red, que ha organizado simposios en 2013 y 2014, y publicado libros con las participaciones en estos. En 2015 está terminando un proceso participativo para producir una declaración conjunta (DCNN, 2015).

La organización mexicana Red de Defensa de los Derechos Digitales (R3D) ha publicado recientemente un estudio sobre las posibles violaciones a la neutralidad de la red en México. Este estudio no pudo documentar violaciones del tipo bloqueo o filtrado de flujos en redes fijas, aunque sí en las móviles, con las herramientas a su alcance. Documentó que los principales operadores tienen convenios y productos al público que hacen tratamiento preferencial para algunos servicios, como los medios sociales; es decir, diversas formas de subsidio o de *zero-rating* (R3D, 2015).

Los OTT que ofrecen estos servicios lo hacen como un *loss leader*: un producto cuyas utilidades pueden ser menores a las regulares o incluso producir pérdidas, para atraer consumidores, como lo ha declarado Mark Zuckerberg (cuyo servicio *zero-rating* pasó de llamarse internet.org a Free Basics, entre otros motivos, debido a las acusaciones de atentar contra la neutralidad de la red). Por otra parte, los operadores de red pueden estar haciendo lo complementario, atraer clientes a sus servicios de paga o tarifa ordinaria cuando los suscriptores salgan de los jardines vedados a la "Internet Abierta".

No existe un consenso global definitivo sobre la bondad de esta práctica ni de su carácter posiblemente violatorio de la

neutralidad de la red (sin dejar de notar los casos chileno y holandés ya mencionados). La legalidad de la práctica deberá ser juzgada país por país de acuerdo con la legislación aplicable. Una revisión del estado del *zero-rating* en cinco países ha sido publicada por Carolina Rossini y Taylor Moore (2015).

5. Conclusiones y recomendaciones

Es importante cambiar la óptica de operación de los prestadores de servicios de telecomunicaciones respecto a los contratos de adhesión de servicios, pues estos reflejan un compromiso laxo con su calidad de servicio, al entregarlo con el concepto de "mejor esfuerzo" que permite todas las prácticas de sobresuscripción y desalienta la actualización tecnológica de los servicios prestados. Los ciudadanos requieren también certezas de la calidad de sus servicios y contar con una base para poder vigilar cualquier violación a la operación abierta de internet.

Es muy importante dejar claro que al hablar de "Internet Abierta" no queremos decir que sea una internet sin fronteras. Las fronteras se relacionan con la capa tres, pues es el derecho legítimo de cada dueño de su red decidir las políticas con las que administra su gestión de tráfico, siempre y cuando se preserve el principio de cooperación en internet, un principio de igualdad en el que no deben existir sesgos o abusos de poder en la transmisión de tráficos ajenos.

Desde este punto de vista técnico, la neutralidad de la red que se demanda en la actualidad es en gran medida una

ficción, pues la neutralidad respecto a orígenes, destinos y contenidos, sin bloqueos ni priorizaciones, no es factible en la práctica. Las políticas de administración son diferentes en cada dominio administrativo, lo cual es una libertad fundamental contra la que no debemos atentar. Cada operador es libre de administrar su red, con las reglas y formas a su alcance económico, técnico y administrativo. Las redes que forman internet son diferentes en anchura de banda, en software, en equipamiento y, como ya dijimos, en reglas de administración. Esta magna cooperación en libertad es la raíz de la explosiva expansión de internet.

En México, el debate entre operadores, OTT, las comunidades técnica y académica, y la sociedad civil podría acercarse próximamente a una conclusión decisiva: no se trata de impedir la gestión de tráfico, pues de entrada es necesaria, como hemos demostrado. Se trata que la gestión se lleve a cabo de la mejor manera posible.

Así, es conveniente enfocar el debate más allá del concepto que apela a la neutralidad de la red en forma absoluta y orientarlo en explorar reglas para la operación y administración de redes basadas en relaciones de certeza y transparencia. En estas reglas se deberán contener previsiones para aceptar que todas las redes en operación son administradas, que la operación debe simular, en lo posible, los efectos de acuerdos de transparencia sobre la neutralidad de la red, respecto a contenidos y las acciones para contener y mejorar los desempeños de las comunicaciones, permitiendo un acceso justo que evite el trato discriminatorio de contenidos.

Se debe evitar la distorsión (por filtrado, bloqueo, *throttling* o estrangulamiento, entre otras conductas conocidas) de contenidos y flujos propios de los operadores o de sus aliados comerciales en demérito del acceso de las personas a sus competidores.

Es importante enfocar a las organizaciones ciudadanas a evitar el abuso de control de los operadores en detrimento de las libertades de acceso a la información, de expresión y de asociación. Cualquier conducta que el Estado o los operadores ejecuten en este sentido deberá ser impedida; cabe mencionar que el tráfico debe ser lícito[9] y no tener impacto amenazador sobre la seguridad y estabilidad de las redes. Los incentivos de los operadores que cuentan con integración entre operación de redes y provisión de contenidos deben ser vigilados especialmente.

Es posible que los consensos viables se basen en una regulación *ex post* y no tan solo en una *ex ante*, que al menos debe contemplar el principio de aplicación de gestión de red no diferenciada por el pago del servicio. La regulación *ex post*, como es común en la regulación de la competencia, se irá conformando con las resoluciones del regulador. En México y otros países, la regulación *ex post* conlleva el riesgo de fracasar en litigios, al reclamar los regulados una falta de certeza jurídica, ausencia del estado de derecho y aplicación retroactiva de la ley.

El regulador y el complejo de actores multisectoriales que

9 Cabe reconsiderar el requerimiento de licitud en el caso de reglas emanadas de dictaduras o no ajustadas a estándares de derechos humanos.

participe en el debate en los años próximos deberá tener una gran fuerza institucional para mantener los mejores beneficios de la neutralidad de la red, en el entendido que su definición misma será cambiante, además de serlo las condiciones técnicas, políticas, comerciales, legales y regulatorias del entorno de internet.

En la legislación actual, la neutralidad de la red ha sido ligada al consumo y solo después como un marco que norme relaciones entre iguales para los que desean expresarse en la red. Esto último cambiará si dejamos de ser exclusivamente usuarios pasivos y pasamos a ser ciudadanos activos en la producción de contenido, servicios e innovación tecnológica.

La defensa de la neutralidad de la red como emblema de la no interferencia de los operadores -y por extensión o de trasmano el Estado- será la bandera viable, siempre evitando el efecto paradójico y preterintencional de una indeseable intervención del Estado en las libertades ciudadanas como ya se ha descrito. El análisis y escalamiento de las campañas puede seguir el esquema propuesto por Pisanty (2013) siguiendo las huellas de las distintas intervenciones como se analiza en el trabajo posterior de Pisanty (2014). La prevención contra campañas mal fundadas técnicamente que ha expresado Huesca (2015) debe ser atendida.

Independientemente del enfoque que finalmente definan las reglas escritas (leyes, reglamentos, acuerdos de los reguladores), la sociedad civil y la comunidad técnica deberán insistir invariablemente en la participación multisectorial en las deci-

siones, utilizando todas las oportunidades legales. Entre esas, deben considerar, además de órganos como el Consejo Consultivo del Instituto Federal de Telecomunicaciones, las instancias consultivas correspondientes de las entidades consagradas a la protección de los consumidores, de la competencia económica y de los derechos humanos. En lo posible, se debe impulsar la creación de consejos ciudadanos y la organización de encuentros multisectoriales que emitan propuestas viables para la construcción de la autorregulación.

Además, las organizaciones interesadas deberán dotarse de las herramientas técnicas de medición más avanzadas y creíbles, difundir su uso y formar redes que permitan detectar y corroborar irregularidades hasta el nivel de carga de la prueba más exigente posible; OFCOM (2015), m-lab (2015) y muchos otros proveen herramientas para este fin. Algunas de estas herramientas deberán ser validadas por el regulador y, de ser posible, por normas Normas Oficiales Mexicanas (NOM) o Normas Mexicanas (NMX).

Arkko, Jari. "RFC Authors by Country contributions". en Distribution of Documents According to the Countries of their Authors, septiembre de 2015. http://www.arkko.com/tools/allstats/d-countrydistr.html (consultado el 16 de diciembre de 2015).

Carpenter, Brian. "Request for Comments (RFC) 1958: Architectural Principles of the Internet". ieft, junio de 1996. https://www.ietf.org/rfc/rfc1958.txt (consultado el 6 de agosto de 2015).

Dynamic Coalition on Network Neutrality (dcnn). "Dynamic Coalition on Network Neutrality Network Neutrality Policy Statement". Internet Governance Forum, 5 de agosto de 2015. http://review.intgovforum.org/igf-2015/dynamic-coalitions/input-document-on-network-neutrality/dynamic-coalition-on-network-neutrality-dcnn/ (consultado el 16 de diciembre de 2015).

The Economist. "A multi-speed Europe-The EU's new Internet rules will hurt European start-ups", 31 de octubre de 2015. http://www.economist.com/news/business/21677175-eus-new-internet-rules-will-hurt-continents-startups-multi-speed-europe (consultado el 4 de 11 de 2015).

European Commission. "The open internet and net neutrality in Europe", abril de 2011. http://eur-lex.europa.eu/

legal-content/EN/TXT/HTML/?uri=URISERV:si0022 (consultado el 6 de enero de 2016).

Huesca, Erik. "Neutralidad de Red, bandera libertaria sin entender". *Virtualis,* Vol. 5, núm. 10 (2014). http://aplicaciones.ccm.itesm.mx/virtualis/index.php/virtualis/article/view/104 (consultado el 9 de agosto de 2015).

Internet Society. "Open Inter-networking: Getting the fundamentals right: access, choice, and transparency", 21 de febrero de 2010. http://www.internetsociety.org/open-inter-networking-getting-fundamentals-right-access-choice-and-transparency (consultado el 16 de diciembre de 2015).

Internet Society. "Policy Briefs: Network Neutrality", 30 de octubre de 2015. http://www.internetsociety.org/sites/default/files/ISOC-PolicyBrief-NetworkNeutrality-20151030.pdf (consultado el 16 de diciembre de 2015).

Layton, Roslyn, "Net Neutrality Regulation and Broadband Infrastructure Investment: How to Make an Empirical Assessment". *Network Neutrality: an Ongoing Regulatory Debate, 2nd Report of the Dynamic Coalition on Network Neutrality,* editador por Luca Belli y Primavera De Filippi, 38-45. 2014 https://docs.google.com/file/d/0B4CMvT0NORh9RHhKa2IybThhR0U/edit (consultado el 16 de diciembre de 2015).

Marcus, J. Scott . "Network Neutrality Revisited: Challenges and Responses in the EU and in the US". Parlamento Euro-

peo, 2014. http://www.europarl.europa.eu/RegData/etudes/STUD/2014/518751/IPOL_STU%282014%29518751_EN.pdf (consultado el 6 de agosto de 2015).

Lemley, Mark & Lawrence Lessig. "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era". *UCLA Law Review*, Vol. 48, 925. 2001.

OFCOM. "Traffic Management Detection Methods & Tools", agosto de 2015. http://stakeholders.ofcom.org.uk/market-data-research/other/technology-research/2015-reports/traffic-management (consultado el 16 de diciembre de 2015).

Pisanty, Alejandro. "Network Neutrality under the Lens of Risk Management". *The value of Network Neutrality for the Internet of Tomorrow: Report of the Dynamic Coalition on Network Neutrality,* editado por Luca Belli y Primavera De Filippi, 61-70. 2013, https://hal.archives-ouvertes.fr/hal-01026096/document (consultado el 16 de diciembre de 2015).

Pisanty, Alejandro. "Network Neutrality Debates in Telecommunications Reform–Actors, Incentives, Risks". *The value of Network Neutrality for the Internet of Tomorrow: Report of the Dynamic Coalition on Network Neutrality,* editado por Luca Belli y Primavera De Filippi, 38-45, 2013 https://docs.google.com/file/d/0B4CMvT0NORh9RHhKa2IybThhR0U/edit (consultado el 16 de diciembre de 2015).

Red en Defensa de los Derechos Digitales (R3D). "Neutralidad de la red en México: del dicho al hecho". http://f.cl.ly/items/3K2T3v0b452g0a1C0d2E/R3D%20-%20Neutralidad%20de%20la%20red%20en%20Mexico%202015.pdf (consultado el 5 de enero de 2016).

Rossini, Carolina y Taylor Moore. "Exploring Zero-Rating Challenges: vies from five countries". Public Knowledge, 28 de julio de 2015. https://www.publicknowledge.org/assets/uploads/blog/Final_Paper-Jul_28-TM.pdf (consultado el 7 de agosto de 2015).

Sorensen, Frode. "How can the Open Internet coexist with new IP services?", Norwegian Communications Authority, 4 de junio de 2015, http://eng.nkom.no/topical-issues/news/how-can-the-open-internet-coexist-with-new-ip-services (consultado el 16 de diciembre de 2015).

Van Schewick, Barbara, *Internet Architecture and Innovation,* Cambridge, MA: mit Press, 2010.

Wu, Tim. "Network Neutrality, Broadband Discrimination", *Journal of Telecommunications and High Technology Law,* Vol. 2, 2003.

Ley Federal de Telecomunicaciones y Radiodifusión, *Diario Oficial de la Federación,* 15 de julio de 2014.

Paradojas del "gobierno abierto" en el contexto mexicano

Juan Manuel Casanueva[1]

La idea de "gobierno abierto" está íntimamente relacionada con el concepto de democracia. Implica el involucramiento pleno de la ciudadanía en el quehacer público y se fundamenta no solo en tener transparencia y rendición de cuentas, sino además en participar activamente en procesos gubernamentales.

Un "gobierno abierto" es uno transparente y democrático, que va más allá de la democracia formal que implica los procesos de voto y legislación, para convertirse en una democracia sustantiva en términos de ejercicio de derechos humanos e involucramiento activo de los ciudadanos en el gobierno (Perez, 2013). Para implementar este concepto, se recurre a mecanismos de apertura, como lo son los acuerdos y compromisos entre ciudadanos, estados y comunidad internacional, con el fin de lograr los objetivos planteados. Vale la pena decir que, en el siglo XXI, los mecanismos para una participación de este tipo pasan inevitablemente por las tecnologías de información y las comunicaciones,

1 Quiero agradecer especialmente a Cynthia Cárdenas por su colaboración en este artículo.

el manejo de datos y el uso de internet (Shkabatur, 2011).

En este sentido, en México vivimos una situación de contradicción permanente: aunque existen un puñado de mecanismos de apertura en acciones concretas, con buenos y sólidos resultados, el gobierno sigue siendo opaco, corrupto, vertical y autoritario (Meyer, 2013).

Por un lado, las estructuras de diálogo que se han generado entre sociedad civil, el órgano garante de transparencia y el gobierno federal, implican muchos avances a nivel de interlocución y creación de políticas para la apertura gubernamental que han derivado en acciones concretas. Pero una segunda arista, de carácter sistémico, excluye la apertura real como característica del Estado mexicano.

No importa cuántos compromisos se asuman ni cuántos mecanismos de apertura se pongan en marcha, los problemas estructurales del Estado mexicano son tan graves que imposibilitan la óptima participación ciudadana en el gobierno. La verdadera apertura solo es posible mediante una transformación de fondo que posibilite el ejercer el derecho a la privacidad, a la libertad de expresión y al acceso a la información, entre otros.

En este sentido, la obligación principal recae en el gobierno a nivel de políticas públicas; pero la sociedad civil también tiene una fuerte responsabilidad. Sobre todo si tomamos en cuenta que los mecanismos de apertura surgen a partir de consensos, compromisos y acuerdos entre ciudadanos, organismos de gobierno y activistas. Si bien desde la sociedad civil se han

construido y mantenido mecanismos de apertura, los temas de derechos digitales relacionados con la privacidad y la vigilancia en línea se han dejado de lado en este proceso.

1. ¿Qué es el "gobierno abierto"?

Daniel Lathrop y Laurel Ruma (2010) definen "gobierno abierto", en su acepción más simple, como el derecho que tiene la gente a acceder a documentos y procedimientos del gobierno. Es decir, la idea de que el público tiene derecho de escrutar a su gobierno, así como participar directamente con él en encuentros que ofrezcan luz y claridad sobre sus procesos. Un "gobierno abierto" debería significar mejoras en la comunicación y operaciones de todas sus ramas, generando mayor eficiencia y mejor rendición de cuentas (o *accountability*).

El objetivo final es que la apertura gubernamental sea una práctica cotidiana en el ámbito federal, estatal y municipal, en los tres poderes del Estado y en otros sectores, como el privado, involucrando al mayor número de actores sociales posible.

Reforzando la definición anterior, Alejandro Pisanty (2013) define gobierno abierto como el conjunto de prácticas por las que los gobiernos democráticos tradicionales se relacionan con los ciudadanos, aplicando los principios de conversación permanente, en sentido doble: hablar, escuchar y responder para conocer sus opiniones y reaccionar ante las mismas, mejorando así la prestación de los servicios y la promulgación de normas.

Pisanty asegura que un "gobierno abierto" lo es no solo en el acceso unidireccional a la información, sino en un diálogo mul-

tidireccional con los actores sociales, a un paso más rápido y en un grano más fino que el que permiten los grandes procesos electorales y legislativos. Un "gobierno abierto" es un gobierno eficaz y transparente, que rinde cuentas con agilidad.

Si bien la idea de "gobierno abierto" está íntimamente relacionada con internet y las tecnologías digitales, no es equivalente a "gobierno electrónico", que busca aprovechar la infraestructura para brindar trámites y servicios a la ciudadanía de forma más eficiente, logrando un segundo nivel de participación. Por ejemplo, el pago de impuestos en línea o registros de cualquier tipo.

A nivel internacional, la principal organización dedicada a impulsar compromisos concretos con la apertura gubernamental es la Alianza para el Gobierno Abierto (OGP, por sus siglas en inglés), surgida en 2011 como una iniciativa multilateral conformada en un principio por ocho países firmantes: Estados Unidos, Gran Bretaña, Noruega, Filipinas, Brasil, Indonesia, Sudáfrica y México.[2]

Desde entonces, la Alianza ha asumido un rol de apoyo y liderazgo de alto nivel, al grado que a 2015, 64 países se han involucrado y asumido compromisos de apertura gubernamental, de la mano con representantes de su sociedad civil.[3]

2 The White House, "The Obama Administration's Commitment to Open Government: Status Report", http://www.whitehouse.gov/sites/default/files/opengov_report.pdf. (consultado el 10 de marzo de 2015) Traducción propia.

3 Alianza para el Gobierno Abierto, "Participating Countries", Open

La Alianza es un acuerdo voluntario entre países, con participación de representantes de la sociedad civil; no es ni un tratado internacional ni una organización internacional propiamente dicha. De acuerdo a su declaratoria, la participación de los gobiernos los compromete a "fomentar una cultura de gobierno abierto que empodere y brinde resultados a los ciudadanos, y promueva los ideales del gobierno abierto y participativo del Siglo XXI". Cada dos años la Alianza organiza una reunión internacional, que en 2015 tuvo lugar en México.

La Alianza basa la apertura gubernamental en cuatro pilares: transparencia, rendición de cuentas, participación ciudadana y tecnologías habilitadoras. Sus integrantes se suman a la Declaratoria de Gobierno Abierto, que a su vez se compromete con la Declaración Universal de los Derechos Humanos, la Convención de las Naciones Unidas contra la Corrupción y otros instrumentos internacionales relacionados con los derechos humanos y el buen gobierno. Esta declaratoria identifica la apertura gubernamental como un proceso que requiere el compromiso permanente y sostenible por parte de los gobiernos,[4] comprometiéndolos a consultar con el público sobre su aplicación y a actualizarse ante desafíos y oportunidades.

Government Partnership, https://www.opengovpartnership.org/es/countries (consultado el 29 de enero de 2016).

4 Alianza para el Gobierno Abierto. "Declaración de Gobierno Abierto", Open Government Partnership, http://www.opengovpartnership.org/es/acerca-de/declaraci%C3%B3n-de-gobierno-abierto (consultado el 29 de enero de 2016).

En particular, los gobiernos establecen su compromiso para:

- Aumentar la disponibilidad de información sobre las actividades gubernamentales.
- Apoyar la participación ciudadana.
- Aplicar los más altos estándares de integridad profesional en los gobiernos.
- Aumentar el acceso a las nuevas tecnologías para la apertura y la rendición de cuentas.

Además existen otros conceptos que son cruciales y hay que tener en mente cuando se habla de gobierno abierto:

- Compromisos de apertura: surgen de acuerdos multisectoriales que, dependiendo de la visión de "gobierno abierto", la agenda temática o de la causa y capacidad de negociación, determinan las acciones a las que el gobierno se compromete.

- Planes de acción: conjunto de compromisos que los gobiernos deben cumplir en un periodo de dos años.

- Datos abiertos: el principio que la información pública debe estar disponible, no solo mediante solicitudes de acceso, sino en páginas de internet con formatos utilizables o formatos abiertos; es decir, un formato digital que permita procesar la información. Por ejemplo, si un artículo está en pdf, está disponible pero no es utilizable; debe estar en formato .ccuv para Excel o .txt genérico de Texto.

Por la conformación de la Alianza y ante la diversidad de

contextos gubernamentales, se optó por no imponer esquemas rígidos a los compromisos de apertura gubernamental. Existen recomendaciones generales, como la *Open Government Guide*,[5] que tiene como función orientar a los procesos de cada país.

En México, desde un inicio existió un proceso de negociación entre la sociedad civil y el gobierno para definir y dar seguimiento a los compromisos de cada uno de los Planes de Acción. Este proceso ha ido cambiando a lo largo del tiempo en un contexto de cocreación. De la misma forma, el órgano de gobernanza multisectorial, conocido como el Secretariado Técnico Tripartita (STT), y los mecanismos de gobierno abierto han evolucionado a través del tiempo.[6]

Desde 2011, México es uno de los países impulsores de la Alianza para el Gobierno Abierto. A nivel país, son tres los actores principales que conforman el STT: el Gobierno Federal, el Instituto Nacional de Acceso a la Información (INAI) y un núcleo de ocho organizaciones de la sociedad civil, que incluye a Artículo19, CIDAC, Cultura Ecológica, Fundar, GESOC, IMCO, SocialTIC y Transparencia Mexicana.

El STT es donde se definen y dan seguimiento a los compromisos de gobierno determinados en los "Planes de Acción". La relación de los representantes del Gobierno Federal, del Instituto Nacional de Acceso a la Información y la sociedad

5 Disponible en http://www.opengovguide.com/?lang=es (consultado el 29 de enero de 2016).

6 *Ibídem.*

civil se da en un contexto de igualdad entre las partes, logrando establecer una relación horizontal que pocos otros países de la Alianza han alcanzado (Barrera, 2015).

En México se han ejecutado dos "Planes de Acción". Un tercero se pondrá en marcha, en teoría, a inicios de 2016.[7] El segundo de ellos, concluyó a fines de 2015 en la Cumbre Global de la Alianza para el Gobierno Abierto celebrada en México. Se anunció el cumplimiento total de los 26 compromisos acordados, incluyendo aquellos que generaron mayores tensiones entre la sociedad civil y las dependencias gubernamentales involucradas, como el Registro de Detenidos, la Base de Datos de Personas Desaparecidas y la

7 El primer Plan de Acción consistió en una serie de más de cuarenta compromisos que el gobierno acordó cumplir entre 2011 y 2012. Cada uno de esos compromisos fue definido a propuesta de las siete organizaciones previamente mencionadas. Por lo tanto, los compromisos varían mucho en naturaleza y alcance. En el "Primer Plan de Acción", el 48 % de los compromisos estuvo relacionado con la eficiencia y eficacia del manejo de recursos y el 29 % al aumento de la integralidad pública. Para el "Segundo Plan de Acción 2013-2015", se establecieron mesas temáticas de trabajo que discutieron y definieron 17 compromisos que debería cumplir el gobierno mexicano, a los que se agregaron otros nueve tras un proceso de consulta gubernamental. En la etapa de seguimiento, cada organización de la sociedad civil mantendría contacto directo con las contrapartes de gobierno correspondientes para evaluar su avance y hacerlo público en sesiones de rendición de cuentas semestrales. Alianza para el Gobierno Abierto, "Reporte de cumplimiento del primer año de trabajo México - 14 de diciembre de 2012", Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, http://aga.ifai.mx/SiteAssets/DocAlianzaMexico/ReportePrimerAño.docx (consultado el 29 de enero de 2016).

Adhesión de México a la Iniciativa de Transparencia de las Industrias Extractivas.[8]

Fuera de la OGP, en México existe la "Alianza para el Parlamento Abierto": una iniciativa formada por grupo formado por doce grupos de la sociedad civil mexicana para impulsar la apertura de la actividad legislativa en la Cámara de Diputados federal, la Cámara de Senadores federal y los Congresos de cada estado del país. A diferencia de la OGP, aún no existe un mecanismo de diálogo y definición de compromisos formal entre sociedad civil y los congresos del país. Este proceso aún es incipiente y mayormente basado en acciones de impulso y análisis de apertura legislativa por parte de sociedad civil.[9]

Sobre este último punto, y como conclusión preliminar, podemos decir que el mecanismo no es solo de consulta y diálogo, sino también de cooperación.

Se ha dicho mucho que los compromisos deberían ser más profundos y ambiciosos (Barrera, 2015). Si bien, en un comienzo los países adoptaron compromisos asociados al gobierno electrónico, acceso a la información y "datos abiertos" –siguiendo tendencias derivadas de los procesos de digitalización y de transparencia en el mundo– a medida que se

8 El reporte completo del cumplimiento del segundo Plan de Acción México se puede encontrar en http://tablero.gobabiertomx.org/ (consultado el 29 de enero de 2016).

9 Más información sobre la Alianza para el Parlamento Abierto puede encontrarse en http://www.parlamentoabierto.mx/

fortaleció la vinculación con la sociedad civil, estos compromisos debieran adquirir características que fomentan la participación ciudadana y la rendición de cuentas de manera más profunda. Esto no está ocurriendo en México: dos de los compromisos adquiridos en el segundo Plan de Acción fueron el Portal de Detenidos y el Padrón de Beneficiarios de Subsidios, que se limitan a poner información de manera pública en internet, sin obligar al gobierno a hacer tareas de comunicación e incidencia para incluir a la ciudadanía en estos temas.

Por su parte, aunque la sociedad civil esté involucrada en la definición y seguimiento del compromiso, su participación está acotada a su área de acción, sin poder hacer campañas que acerquen a los ciudadanos a dichos portales y mecanismos.

2. Gobierno Abierto y Derechos Humanos

Para lograr un gobierno verdaderamente abierto, además de generar mecanismos de transparencia y rendición de cuentas del trabajo de la autoridad, debe existir un adecuado marco para el ejercicio de los derechos humanos, tanto en línea como en el mundo analógico. Sin un piso sólido en este sentido, no se pueden tener las condiciones para un ejercicio pleno de la democracia.

Tres son los factores que más preocupan en este ámbito. El primero es el del derecho a la privacidad, principalmente ante la inminente incongruencia evidenciada por las revelaciones de espionaje masivo realizadas en secreto por países involucrados en procesos de gobierno abierto. El segundo son las condiciones de libertad de expresión y participación

segura de la población en debates de interés público. Y el tercero corresponde a la extensión legal y práctica en torno al acceso a datos abiertos, información, conocimiento y uso.

En materia de derechos digitales, México aún no ha planeado mecanismos para su defensa y promoción en los marcos actuales de los procesos de apertura, ni desde gobierno ni desde la sociedad civil.

2.1 Derecho a la privacidad

En principio, la legislación mexicana protege la privacidad, reconociéndola como derecho y sancionando penalmente algunos actos que la vulneran. Asimismo, las leyes actuales relacionadas a datos personales restringen el acceso y uso no consensuado de información personal por parte de entidades privadas.

Sin embargo, en materia de vigilancia, el resguardo legal de la privacidad es más laxo. Tanto el nuevo Código Nacional de Procedimientos Penales como la Ley de Telecomunicaciones y Radiodifusión, relajaron las condiciones para la intervención de comunicaciones privadas por parte del Estado. Además, las revelaciones de Hacking Team pusieron de manifiesto los mecanismos de espionaje del gobierno mexicano hacia sus ciudadanos y opositores políticos.[10]

10 Ernesto Aroche. "El gobierno de Puebla usó el software de Hacking Team para espionaje político", *Animal Político,* 22 de julio de 2015, http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/ (consultado el 29 de enero de 2016).

Hoy, en virtud del Código Nacional, distintas autoridades como la Procuraduría General de la República, las procuradurías estatales y los ministerios públicos tienen facultades para solicitar la intervención de comunicaciones privadas sin necesidad de la autorización judicial. El limitar la decisión judicial sobre la intervención de comunicaciones elimina los controles necesarios que obligan a las procuradurías a que sustenten sus casos de investigación y da pie a un uso arbitrario de la medida.[11]

Por otro lado, la Ley de Telecomunicaciones y Radiodifusión amplió las medidas de acceso a las comunicaciones y datos de individuos por parte de autoridades con competencias en seguridad pública, además de obligar a los operadores de telecomunicaciones a retener los datos de actividad de sus usuarios para cooperar con la autoridad judicial. En este sentido, faltan controles precisos y mecanismos de transparencia que establezcan salvaguardas para inhibir el abuso de las medidas de vigilancia como lo son la transparencia, la supervisión independiente o la notificación al afectado: todos estos, principios corales de la idea de "gobierno abierto".[12]

A lo anterior se suma la exposición de documentos de la empresa italiana de espionaje digital, Hacking Team, que evidencia contratos de compra y negociaciones con dependencias federales y

11 Para mayores detalles, véase, en este mismo volumen, el capítulo sobre vigilancia estatal de Luis Fernando García y Jesús Robles Maloof.

12 El texto completo de la Ley Federal de Telecomunicaciones y Radiodifusión puede ser encontrado en http://www.sct.gob.mx/fileadmin/Comunicaciones/LFTR.pdf

estatales en todo el país. Considerando las funcionalidades de la tecnología adquirida, existe la sospecha que se pueda estar utilizando de manera abusiva sobre la ciudadanía, aun sin la presunción de su involucramiento en actividades criminales, particularmente activistas, periodistas y defensores de derechos.[13]

Si la idea de gobierno abierto parte de la horizontalidad entre el gobierno y los ciudadanos, el espionaje y la vigilancia arbitraria rompen con este principio para implementar una política vertical carente de cualquier tinte igualitario. ¿Cómo se pueden asegurar las necesarias condiciones de participación, si la ciudadanía no tiene certeza del actuar de su gobierno ni cuando su espionaje es desmedido? ¿Cómo garantizar la participación libre cuando una de las partes puede observar la conducta privada de la otra?

El 17 de diciembre de 2013, un grupo de más de cien organizaciones civiles, grupos de derechos humanos, académicos y ciudadanos enviaron una carta a todos los gobiernos que conforman la Alianza por el Gobierno Abierto para manifestar su preocupación con respecto a la vigilancia masiva. El punto central de este documento es que la hipótesis de apertura es incompatible con la vigilancia de un Estado a sus ciudadanos.[14]

En el texto, dirigido a los copresidentes de la Alianza, entre los

13 Véase la obra citada de Luis Fernando García y Jesús Robles Maloof.

14 "Letter to OGP governments", Open Government Partnership Blog, http://www.opengovpartnership.org/blog/blog-editor/2013/12/20/letter-ogp-governments (consultado el 29 de enero de 2016).

cuales se encuentra un representante de México, se lee el reclamo a la intercepción rutinaria de las comunicaciones privadas por parte de varios gobiernos miembros de la Alianza, considerando que estas prácticas tienen un efecto profundamente negativo sobre la libertad de expresión, información y asociación, sin la cual los ideales de un gobierno abierto no tienen ningún significado.

Los firmantes de esta carta solicitaron que los gobiernos miembros de la Alianza cumplieran con lo siguiente:

- Reconocer la necesidad de actualizar el entendimiento y la situación de la ley que ampara la privacidad y los derechos humanos, para que contemple tecnologías y técnicas actuales de vigilancia.
- Como parte de sus Planes de Acción, comprometerse a la revisión de las leyes nacionales, con el propósito de definir las reformas necesarias para regular el legítimo y proporcional involucramiento del Estado en la vigilancia de las comunicaciones, garantizar la libertad de prensa y proteger a informantes o denunciantes (*whistleblowers*) que comuniquen los abusos del poder del Estado. El plazo otorgado para esto era octubre de 2014.
- Comprometerse a transparentar los mecanismos de vigilancia, la exportación de tecnología para la vigilancia, el apoyo dirigido a la implementación de tecnologías de vigilancia y los acuerdos para compartir datos de la ciudadanía entre estados.

El plazo solicitado pasó sin avances en la revisión normativa. El gobierno mexicano no ha dado ninguna respuesta

ante el llamado de diversas organizaciones de la sociedad civil internacional respecto a la intercepción rutinaria de las comunicaciones privadas.

Así las cosas, México carece de normativa para transparentar los mecanismos de vigilancia, la importación de tecnología para la vigilancia, el apoyo dirigido a la implementación de tecnologías de vigilancia y los acuerdos para compartir datos de la ciudadanía entre estados. Tampoco ha mostrado compromiso en los espacios de gobierno abierto para dar luces sobre esos procesos.

2.2. Condiciones para la participación ciudadana

Uno de los cuatro pilares para la apertura gubernamental, basado en la Alianza de Gobierno Abierto, es la participación ciudadana. Sin involucramiento y participación ciudadana en las decisiones y acciones del gobierno, no hay apertura gubernamental. Si bien existe una amplia gama de visiones en torno a la participación ciudadana que definen los estímulos, precondiciones y naturaleza de la misma, con base en la práctica se señala que la ciudadanía debe ser capaz activamente de proponer, construir y vigilar las acciones gubernamentales que le atañen en todos los ámbitos de gobierno.

En este proceso, es fundamental que la ciudadanía tenga información accesible y utilizable a través de plataformas idóneas para su uso y entendimiento. De ahí la relevancia del uso de nuevas tecnologías de la información y comunicación, así como la publicación de datos abiertos en todos los ámbitos de la apertura gubernamental.

Los países involucrados en procesos de apertura gubernamental que tienen altos índices de violencia, impunidad y violaciones sistemáticas a los derechos humanos, enfrentan una incongruencia que tiene consecuencias prácticas en los niveles de participación ciudadana. A medida que las acciones de participación son influenciadas por el miedo, las limitantes a la libertad de expresión y las estructuras de coerción inhiben la participación, aún cuando exista información disponible en formatos abiertos.

México es una gran paradoja en este sentido. Por un lado, mecanismos como el Plan Nacional de Datos Abiertos (cuyo borrador fue puesto en línea para recibir evaluaciones y comentarios ciudadanos) constituyen una innovación y ejemplo a nivel mundial en cuanto a "gobierno abierto". Sin embargo, en cuanto a los derechos y condiciones de la participación ciudadana, México vive un contexto con amplias limitantes, tanto en plano analógico como en el digital.

La libertad de expresión ha sido severamente coartada en el país, tal como señalan los informes de Article 19, Freedom House y la Comisión Nacional de Derechos Humanos. Periodistas, grupos de activistas y defensores de derechos humanos son rutinariamente amenazados y víctimas de agresiones físicas y psicológicas. La libertad de prensa en México está limitada por el miedo, la impunidad y la violencia.

En su informe de 2015, Article 19 registró 59 agresiones por medio de plataformas digitales; en específico, se registraron 12 ataques cibernéticos a medios de comunicación

con línea editorial crítica al gobierno. También se identifica a autoridades gubernamentales como fuente de cerca de la mitad de los casos de agresión a periodistas en el país.[15]

Estos grupos activos de la sociedad experimentan miedo y es común identificar autocensura. En el plano cívico, en las zonas más conflictivas del país, reporteros ciudadanos y blogueros han sido víctimas de amenazas, acoso, agresiones y hasta asesinatos por difundir información sobre situaciones de corrupción y crimen organizado. Casos como el asesinato de tuiteros en Tamaulipas en 2011 o las recompensas para quien aportara datos de las personas detrás del sitio *Valor por Tamaulipas* en 2013, han marcado los niveles de gravedad a la expresión cívica de los últimos años.[16]

En un contexto de violencia, desconfianza en las autoridades e impunidad como el que existe en México, resulta riesgoso llevar procesos de apertura gubernamental de profundidad en materia de seguridad pública, justicia y

15 Article 19, "Estado de censura", https://www.article19.org/data/files/media library/37906/EstadodeCensuraIntro.pdf (consultado el 29 de enero de 2016).

16 Freedom House "Informe sobre la libertad de prensa: Capítulo México", 2014, https://freedomhouse.org/sites/default/files/Mexico%20 LibertadPrensa2014.pdf (consultado el 29 de enero de 2016) y Mari Luz Peinado, "El narco mexicano pone precio a la cabeza de un tuitero: 36.000 euros", *El País*, 14 de febrero de 2013, http://internacional.elpais.com/internacional/2013/02/14/actualidad/1360875130_983465.html (consultado el 29 de enero de 2016).

demás ámbitos. Tal apertura exige visibilizar e involucrar a la ciudadanía –tanto en línea como en el mundo analógico– en estructuras gubernamentales infiltradas por la corrupción y el crimen organizado (Cuéllar, del Río y Yáñez, 2013).

A consecuencia de lo anterior, y bajo el indignante contexto de la desaparición de 43 estudiantes normalistas de Ayotzinapa en septiembre de 2014,[17] al inicio del Encuentro Regional de las Américas de la Alianza por el Gobierno Abierto en San José, Costa Rica, el 17 de noviembre 2014, el núcleo de la sociedad civil mexicana en OGP manifestó su descontento y expectativa al gobierno mexicano:

> México, como presidente de esta Alianza, debe fungir como ejemplo para los demás países y garantizar una relación de diálogo verdadero entre todos los órdenes de gobierno, poderes y la sociedad. La fragmentación existente entre las partes hace imposible que funja como guía y dé cumplimiento a los objetivos de esta iniciativa. Por esto, organizaciones de la sociedad civil, académicos, activistas, programadores y desarrolladores de México y de las Américas se solidarizan con las familias de los jóvenes desaparecidos y con la sociedad mexicana y llaman al Gobierno mexicano a mostrar un verdadero compromiso con el gobierno abierto […] La indignación y el dolor no nos van a vencer. Es hora de

17 *El País*, "Ayotzinapa: El caso que oscureció México", 8 de noviembre de 2014, http://elpais.com/tag/matanza_estudiantes_normalistas_iguala/a/ (consultado el 29 de enero de 2016).

que el Estado sepa que no toleraremos ni una simulación más. México necesita un cambio profundo.[18]

En el plano de los derechos digitales, el país no ha emprendido acciones profundas, normativas u operativas para garantizar la libertad de prensa, la plena expresión cívica y la protección de informantes o denunciantes (*whistleblowers*) que comuniquen públicamente los abusos de poder.

2.3. Datos, información y conocimiento abierto

Uno de los fundamentos operativos del "gobierno abierto" es la transparencia activa: que la información esté disponible fácilmente y en formatos accesibles para potenciar el acceso y uso de ella por parte de la ciudadanía. De esta forma, el gobierno debe fomentar la apertura de datos de manera proactiva y amparada en normatividad que garantice la publicación de datos en formatos abiertos, así como el libre uso y reuso de la información pública.

Más allá de los datos abiertos, el concepto general de acceso a los bienes intangibles se asocia al conocimiento y la cultura abierta, como conceptos dotados de interacción con los intangibles disponibles. No obstante, mientras definiciones generales del conocimiento abierto han influenciado definiciones particulares que detallan niveles de disponibilidad, dentro de las comunidades de "gobier-

18 Transparencia Mexicana, "Demanda sociedad civil de las Américas al gobierno mexicano garantizar espacios de confianza con su ciudadanía", 17 de noviembre de 2014, http://www.tm.org.mx/comunicado-ayotzinapa/ (consultado el 29 de enero de 2016).

no abierto", se ha sido poco enfático respecto a ciertos tipos de información y conocimiento que el Estado genera directa o indirectamente. Así, políticas y mecanismos de acceso abierto a la cultura, ciencia y educación aún permanecen ajenos a las comunidades de "gobierno abierto", circunscribiéndose su acción a la información sobre gestión gubernamental.

Los datos abiertos han sido el mecanismo base para fomentar la disponibilidad de la información pública en formatos que permitan ser leídos y utilizados por sus usuarios. Como producto del compromiso gubernamental para el diseño e implementación de una Política Nacional de Datos Abiertos, el gobierno mexicano, por medio de un decreto presidencial, ha definido claramente dos conceptos base:

- Datos abiertos: los datos digitales de carácter público que son accesibles en línea y pueden ser usados, reutilizados y redistribuidos, por cualquier interesado.

- Formatos abiertos: el conjunto de características técnicas y de presentación que corresponden a la estructura lógica usada para almacenar datos en un archivo digital, cuyas especificaciones técnicas están disponibles públicamente, que no suponen una dificultad de acceso y que su aplicación y reproducción no estén condicionadas a contraprestación alguna.[19]

19 "Decreto por el que se establece la regulación en materia de Datos Abiertos", Duario Oficial de la Federación, 20 de febrero de 2015, http://www.dof.gob.mx/nota_detalle.php?codigo=5382838&fecha=20/02/2015

De la misma manera, los datos deben ser gratuitos, no discriminatorios, de libre uso, legibles por máquinas, permanentes y completos.

De forma congruente con la definición y el concepto, también se ha instaurado una "licencia de libre uso que habilita el uso y reuso de la información pública"[20] en formatos abiertos, conforme a lo siguiente:

a. Hacer y distribuir copias del conjunto de datos y su contenido.
b. Difundir y publicar el conjunto de datos y su contenido.
c. Adaptar o reordenar el conjunto de datos y su contenido.
d. Extraer total o parcialmente el contenido del conjunto de datos.
e. Explotar comercialmente el conjunto de datos y su contenido.
f. Crear conjuntos de datos derivados del conjunto de datos o su contenido.

Una definición más amplia de conocimiento abierto es aquella que no solo se refiere a la apertura de datos, sino que incluye las obras producidas o generadas por individuos u organizaciones. Para la Open Definition, el conocimiento es abierto cuando "cualquier persona es libre para acceder,

---

(consultado el 29 de enero de 2016).

20 Esta licencia es compatible con Creative Commons Atribución BY. Los detalles de la licencia pueden encontrarse en http://datos.gob.mx/libreusomx/

usar, modificar y compartir bajo condiciones que, como mucho, preserven su autoría y su apertura".[21] Dicho concepto aplica tanto para los datos de gobierno, como a las obras originadas de acciones o de recursos públicos. Con base en las definiciones de conocimiento abierto, ramas más amplias se están gestando en diversos países fomentando la ciencia, educación y cultura abierta.

En México se promulgó la Ley de Ciencia y Tecnología, donde se abre la posibilidad para que obras académicas financiadas por el Estado mexicano sean puestas a disposición del público a través de repositorios en línea.[22] Si bien es un avance importante en materia de propiedad intelectual y cultura abierta, esta normativa carece de obligatoriedad, por lo que queda a discreción de las instituciones educativas y académicas.

Sin embargo, no porque exista toda una compleja normativa al respecto, significa que hay un verdadero uso libre de estos datos. La expectativa es que el gobierno sea consecuente con sus acciones y fomenten una apertura real. Esto incluye la puesta a disposición de información y la utilización de formatos que faciliten la reutilización de los datos, pero también incluye la formación de capacidades para que el aprovechamiento de esa información no se radique en ciertos

21 "Definición de Conocimiento Abierto", *Open Definition,* http://opendefinition.org/od/2.0/es/ (consultado el 29 de enero de 2016).

22 Ver el Artículo 14 de la Ley de ciencia y tecnología, disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/242_081215.pdf (consultado el 29 de enero de 2016).

grupos o instituciones de manera excluyente, sino que sirva como herramienta de empoderamiento civil.

Incluye, asimismo, la construcción de capacidades en el propio Estado para la continua puesta a disposición, pero también para el uso de la información de manera óptima. Finalmente, incluye también el aseguramiento de mecanismos de rendición de cuentas que permitan adoptar medidas a partir de la información disponible, otorgando a la ciudadanía un efectivo rol contralor del poder.

3. Conclusión: la paradoja mexicana

La apertura gubernamental en México se define por sus acciones, tanto en los procesos formales como los acordados ante la Alianza para el Gobierno Abierto, como también por los contextos que definen la vida diaria en el país. México ha sido capaz de establecer mecanismos para definir y dar seguimiento a compromisos puntuales que aportan significativamente a la apertura gubernamental en muchas áreas de la sociedad, a través del trabajo conjunto del gobierno, la sociedad civil y el órgano garante de acceso a la información.

No obstante estos avances programáticos, el gobierno mexicano dista mucho de realizar ajustes estructurales que modifiquen el operar gubernamental vertical, opaco y limitante de aspectos básicos para la expresión y la participación cívica.

El gobierno mexicano no solamente es opaco, sino que ha intentado engañar a la ciudadanía en una serie de materias relevantes. Un buen ejemplo de ello es la investigación

realizada por la Secretaría de Gobernación para aclarar la desaparición de los 43 normalistas de Ayotzinapa en Guerrero: el gobierno no solo ha sido reacio a entregar la información que públicamente se la ha exigido, bajo el mandato de Jesús Murillo Karam se presentaron evidencias y hechos como una "verdad histórica", prontamente desmentida por investigaciones independientes.[23] Sin embargo, se crea la Base de Datos de Personas Desaparecidas en el marco de Open Government Partnership, tratando de justificarlo como un avance democrático.[24]

En el plano de política económica, México acató los acuerdos de secreto establecidos en las negociaciones del Tratado Transpacífico (TPP). En contra del discurso de transparencia y "gobierno abierto", y a las exigencias de grupos de la sociedad civil nacional e internacional, el gobierno mexicano mantuvo inaccesible el texto del tratado a la ciudadanía, el poder legislativo e incluso a representantes del mismo gobierno. Distinto es el caso de los representantes del sector privado, que sí tuvieron acceso al texto y cabildeo para lograrlo. Esto constituye un desequilibrio de participación diametral.

23 Grupo Interdisciplinario de Expertos Independientes (GIEI), *Informe Ayotzinapa: Investigación y primeras conclusiones de la desapariciones y homicidios de los normalistas de Ayotzinapa,* https://drive.google.com/file/d/0B1ChdondilaHNzFHaEs3azQ4Tm8/view (consultado el 29 de enero de 2016).

24 Secretaría de Gobernación. *Registro Nacional de Desaparecids*. http://secretariadoejecutivo.gob.mx/rnped/consulta-publica.php (consultado el 29 de enero de 2015).

El anterior es otro ejemplo de las importantes contradicciones entre la naturaleza de un gobierno abierto y las acciones del gobierno mexicano. Por más que se cumplan los compromisos ante la Alianza para el "gobierno abierto", será difícil afirmar la apertura gubernamental si son estas mismas instancias gubernamentales las que se niegan a entregar la información, promueven la vigilancia masiva carente de controles y construyen las barreras que limitan la expresión y la participación ciudadana.

Dado que el proceso de "gobierno abierto" es de cocreación y ha tenido una aparente evolución sólida en México, puede constituirse como un espacio para que la sociedad civil aborde las problemáticas de derechos humanos y derechos digitales, que hasta ahora se han quedado fuera de la discusión.

Así como el gobierno debe enfrentar sus contradicciones estructurales y prácticas, también la sociedad civil debe identificar el valor de los espacios formales de participación, incidencia y coconstrucción en la transformación gubernamental y la promoción de los derechos digitales.

4. Recomendaciones de política pública para un "gobierno abierto"

Si el gobierno abierto va a trascender compromisos asociados a acciones o proyectos puntuales, el gobierno, la sociedad civil y la misma Alianza deben realizar ajustes esenciales para que la apertura sea intrínseca a la cultura de gobierno. Para ello, a continuación se resumen las siguientes recomendaciones de política pública.

Primero, al Estado le corresponde el cumplimiento cabal de los derechos humanos. En cuanto al derecho a la libertad de expresión, íntimamente relacionado con el concepto de democracia, es necesario velar para que pueda ser ejercida plenamente en México. Solo de esta forma será posible involucrar a la ciudadanía en los mecanismos de participación, consulta, vigilancia y co-construcción de soluciones para las problemáticas más graves que vive el país.

Tanto en los planos físicos como digitales, es imperativo que el gobierno salvaguarde los derechos de sus ciudadanos y que cambie la cultura institucional para no ser copartícipe de acciones de censura, agresión y abuso en contra de grupos ciudadanos, a costa del respeto del estado de derecho. El respeto a los derechos humanos es condicionante para la participación ciudadana.

En cuanto al derecho a la privacidad, México necesita una ley detallada que establezca mecanismos de transparencia ante las acciones de vigilancia estatal, incluyendo la definición de controles y documentación para evitar su uso arbitrario. Ésta, es una facultad legal de ciertas dependencias de gobierno, por lo que debe garantizarse que sean ellas, y ninguna otra, quienes adquieran y utilicen tecnología, de manera selectiva, para estos fines, relacionados con investigaciones criminales sustentadas y avaladas judicialmente.[25] En el contexto del "gobierno abierto",

25 Para mayor detalle en estas recomendaciones, véase el capítulo de este mismo volumen sobre vigilancia estatal.

esta necesidad es totalmente compatible con mecanismos de contraloría ciudadana.

En cuanto a la protección de datos personales, la legislación mexicana se limita a la posesión y uso de datos en el sector privado. Hasta ahora no existen normas que se refieran a la protección de los mismos por parte del gobierno y las dependencias gubernamentales del poder ejecutivo, legislativo y judicial. Pero es importante que tales reglas existan: el manejo de información personal por parte del Estado debe estar sujeto a límites legales que impidan la afectación de derechos fundamentales por medio del uso de esos datos.

Por su parte, en un país con altos índices de corrupción como México, la protección de denunciantes o *whistleblowers* es esencial. Es necesario que se consideren mecanismos de protección a denunciantes que decidan hacer pública información de interés en aras de la transparencia y rendición de cuentas, tanto en el sector público como en el privado. Esto implica mecanismos efectivos de protección de fuentes periodísticas, pero también protección para aquellos medios que hacen pública información socialmente relevante.

Un tercer punto concerniente al Estado se refiere al mejoramiento de condiciones estructurales, como la impunidad y la inseguridad. No hay participación democrática cuando hay altos índices de criminalidad sin que se ejerza justicia.

El contexto de impunidad de México no solo ha vulnerado el estado de derecho, sino que ha deteriorado el tejido social y las estructuras institucionales, favoreciendo condiciones

de corrupción, concentrando las estructuras arbitrarias de poder y aumentando el uso de la violencia como resolución de conflictos. A medida que exista impunidad, será imposible establecer las condiciones necesarias para que la ciudadanía confíe en las instituciones de gobierno y exista un clima seguro para su participación cívica, y por lo tanto un involucramiento real de la ciudadanía en un contexto de gobierno abierto.

Es fundamental que el Estado sea capaz de asegurar paz y seguridad, dentro y fuera del entorno en línea. Solo cuando un ciudadano o ciudadana es capaz de dar la cara, salir a la calle y expresarse sin temor a represalias, es cuando una plena participación es alcanzable.

Por último, en cuanto al conocimiento abierto en el plano estatal, existen ya pasos sólidos en la Ley de Libre Uso para que el conocimiento público esté disponible de manera gratuita, detallada, proactiva y en formatos utilizables en internet. Sin embargo, se necesita ir más allá: el Estado debe asegurar el licenciamiento abierto a contenidos derivados de financiamiento público, como la derivada de la investigación en materia de educación, ciencia y cultura, por nombrar algunos.

Para una sólida construcción de políticas públicas en el país, también es fundamental la participación activa de la sociedad civil. A nivel nacional, el mecanismo de la Alianza para el Gobierno Abierto permite establecer y dar seguimiento a compromisos gubernamentales. La participación en estos procesos de especialistas y organizaciones de las sociedad

civil permitirá que las problemáticas relacionadas con derechos digitales sean identificados. Asimismo, en los nuevos espacios de diálogo para la apertura gubernamental a nivel de los estados federados, la presencia de especialistas y organizaciones de la sociedad civil determinará las agendas locales. Dado el involucramiento del Instituto Nacional de Acceso a la Información en estos procesos, existe una oportunidad para ampliar la influencia entre los órganos de transparencia estatales. En este contexto, uno de los temas fundamentales es el seguimiento a la compra y uso de tecnología para vigilancia, que debe ser parte de los debates sobre la apertura gubernamental a nivel estatal y local.

En segundo lugar, debemos difundir información y generar capacidades para el análisis sobre la apertura gubernamental bajo una perspectiva de derechos digitales. En este rubro, es cada vez más necesario realizar acciones de información y sensibilización a actores involucrados en los procesos de apertura, de modo que se identifiquen contextos de vulnerabilidad de derechos y se evalúen como parte de las condiciones para la participación ciudadana.

Por otro lado, se requiere monitorear el avance de los compromisos de apertura a nivel nacional y de cada Estado, para poder aportar sus recomendaciones, identificar riesgos, señalar acciones contraproducentes y generar acciones de presión ante legislación, proyectos y acciones gubernamentales reversivas.

A la Alianza le corresponde llevar a cabo varias reformas que eleven los estándares democráticos del "gobierno abierto":

Primero, la modificación de los criterios de aceptación a la OGP, pues estos han sido muy bajos. Esta laxitud ha permitido que países con carencias importantes en materia de transparencia, rendición de cuentas y condiciones para la participación ciudadana, abanderen el concepto de la apertura gubernamental sin realizar cambios significativos en sus acciones.

Los criterios contemplados en la guía de implementación de "gobierno abierto" deben considerarse como requisito para que un país ingrese y permanezca en OGP. Algunas de las temáticas transversales pueden ser: contar con una ley de acceso a la información, regulación para habilitar la participación ciudadana, mecanismo de involucramiento de la ciudadanía en reformas públicas, legislación de privacidad y protección de datos personales y regulación de poderes de gobierno relativos a vigilancia.[26] No se trata de excluir a países que no tengan actualmente ciertos niveles de apertura, sino de exigir compromisos serios hacia una mayor transparencia y participación.

Por último, se deben considerar de manera formal condicionantes relativos a derechos humanos, acceso a la justicia y libertad de prensa para determinar la permanencia de países en la AGA, otorgando un significado real a su propia existencia y al valor de la apertura en los gobiernos.

5. Consideraciones finales

Si la idea de "gobierno abierto" implica el involucramiento

26 Estas temáticas esenciales fueron identificadas de acuerdo a los *cross cutting topics* de la Open Government Guide, disponible en http://www.opengovguide.com

pleno de la ciudadanía en el ámbito público y la participación activa en procesos gubernamentales, la noción misma de democracia se profundiza.

Es cierto que en el siglo XXI los mecanismos para una participación de este tipo pasan inevitablemente por las tecnologías de la información y comunicaciones. Sin embargo, el hacer énfasis en estas últimas –descuidando los procesos de democracia sustantiva en el país–no bastan para lograr una plena participación ciudadana y un cambio en el gobierno. La tecnología en este sentido no puede ser un fin en sí mismo, sino un medio que acompañe procesos sólidos en términos de derechos humanos, para que avancemos en la construcción de un ideal democrático que vaya más allá de "soluciones" tecnológicas a corto plazo.

La obligación principal recae en el gobierno a nivel de políticas públicas, pero también en la sociedad civil. Los mecanismos de apertura surgen a partir de consensos, compromisos y acuerdos entre la ciudadanía, organismos de gobierno y activistas dedicados al tema. Lamentablemente, hoy en México no están garantizadas las condiciones estructurales a nivel de derechos humanos necesarios para que la participación ciudadana sea óptima y podamos hablar de un gobierno realmente abierto.

Alianza para el Gobierno Abierto. "Declaración de Gobierno Abierto", Open Government Partnership, México, 2011. http://www.opengovpartnership.org/es/acerca-de/declaraci%C3%B3n-de-gobierno-abierto

Aroche, Ernesto. "El gobierno de Puebla usó el software de Hacking Team para espionaje político. *Animal Político,* 22 de julio de 2015. http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/

Barrera, Lourdes. "La Alianza para el Gobierno Abierto, una visión desde sociedad civil". México: Alianza para el Gobierno Abierto en México, 2015. http://gobabiertomx.org/wp-content/uploads/2015/10/alianzagobierno.pdf

Freedom House. "Informe sobre la libertad de prensa: Capítulo México", México, 2014 https://freedomhouse.org/sites/default/files/Mexico%20LibertadPrensa2014.pdf

Gutiérrez Cuéllar, Paola y Gabriela Magdaleno del Río. "Violencia, Estado y crimen organizado en México", *El Cotidiano*, México, 2010.

Lathrop, Daniel y Laurel Ruma. *Open Government.* California: O'Reilly Media, Inc., 2010.

Meyer, Lorenzo. *Nuestra tragedia persistente: la democracia autoritaria en México.* México: Debate 2013.

OGP. "Letter to OGP governments", Open Government Partnership Blog, Estados Unidos, 2013 http://www.opengovpartnership.org/blog/blog-editor/2013/12/20/letter-ogp-governments

Perez, Oren. "Open Government, Technological Innovation, and the Politics of Democratic Disillusionment: (E-)Democracy from Socrates to Obama". Israel, 2013.

Peinado, Mary Luz. "El narco mexicano pone precio a la cabeza de un tuitero: 36.000 euros". *El País*, 14 de febrero de 2013. http://internacional.elpais.com/internacional/2013/02/14/actualidad/1360875130_983465.html

Pisanty, Alejandro. "Diagnóstico Agenda Digital y Gobierno Abierto. Alianza para el Gobierno Abierto". México: Alianza Para el Gobierno Abierto, 2013. http://aga.ifai.mx/Noticias/CodeArt_ListPermissionExtension/Diagno%CC%81stico%20Agenda%20Digital%20y%20Gobierno%20Abierto.docx.

Shkabatur, Jennifer. "Digital Technology and Local Democracy in America", Estados Unidos, 2011.

Autores & Autoras

En defensa del anonimato

Antonio Martínez Velázquez. Abogado especialista en derechos digitales y activista a favor de la libertad de expresión. Fue fundador del Partido Pirata Mexicano, que busca una reforma integral al régimen de propiedad intelectal, y miembro fundador de la corriente de opinión de izquierda "Democracia Deliberada". Trabajó como encargado del programa digital en Artículo 19. Actualmente es cofundador de Horizontal.mx, un nuevo medio de crítica cultural.

José Flores Sosa. Maestro en Comunicación y Medios Digitales por la Universidad de las Américas Puebla. Actualmente es director de comunicación de R3D: Red en Defensa de los Derechos Digitales; editor del boletín *Digital Rights Latin America and the Caribbean*; y miembro de la junta directiva de Wikimedia México.

La violencia de género en México y las tecnologías de la información

Estefania Vela Barba. Es abogada del Instituto Tecnológico Autónomo de México y maestra en derecho por la Universidad de Yale. Trabaja como profesora asociada del Centro de Investigación y Docencia Económicas, donde es responsable del área de Derechos Sexuales y Reproductivos. Escribe semanalmente en el periódico *El Universal*, en un blog llamado Pornucopia y ha publicado en *Letras Libres* y *Nexos*.

Erika Smith. Es maestra en estudios de América Latina de la Universidad de Wisconsin. Tiene más de 20 años de experiencia como capacitadora en temas de seguridad y privacidad en internet desde una perspectiva de género. Coordina el proyecto "Basta ya: derechos de las mujeres y seguridad digital" en México, del Programa de los Derechos de las Mujeres de la Asociación para el Progreso de las Comunicaciones (APC), y forma parte de de la coordinación global de la campaña internacional "¡Dominemos la Tecnología!" que acompaña los 16 días de activismo en contra de la violencia de género en línea.

La criminalización de la protesta social digital

Alberto Lujambio Llamas. Activista y egresado de la carrera de derecho del Instituto Tecnológico Autónomo de México. Fue coordinador del libro *Derecho Penal a Juicio,* que reúne varios temas controversiales en el derecho penal mexicano. Actualmente, es director de operaciones de Novelistik: plataforma social de lectura y publicación de libros electrónicos.

José David Aroesti. Estudió la carrera de derecho en el Instituto Tecnológico Autónomo de México y ha ejercido diversos cargos en el Instituto Nacional Electoral y la Procuraduría General de la República. Formó parte del Google Development Group en México. Es programador de sistemas de software y de inteligencia artificial. Actualmente se desempeña como director de tecnología en Novelistik.

La vigilancia y su impacto en el derecho a la privacidad en México

Jesús Robles Maloof. Defensor de derechos humanos, abogado, maestro en humanidades con estudios de doctorado en derechos fundamentales. Desde el 2010, defiende casos de libertad de expresión y derechos digitales. Participa en los colectivos por la libertad en internet: Contingente Mx y Enjambre Digital. Es Senior Lawyer en New Media Advocacy Project México.

Luis Fernando García. Licenciado en Derecho por la Universidad Iberoamericana. Es candidato a Maestro en Derecho Internacional de los Derechos Humanos y Derechos de Propiedad Intelectual por la Universidad de Lund en Suecia. Colaboró en el Departamento de Derechos Humanos y Empresas del Centro Danés de Derechos Humanos. Fue Google Policy Fellow en la Asociación por los Derechos Civiles de Argentina. Es profesor da Universidad Iberoamericana y director de la Red en Defensa de los Derechos Digitales (R3D).

Neutralidad de la red e internet en México: una perspectiva sociotécnica

Alejandro Pisanty Baruch. Realizó sus estudios de licenciatura y posgrado en Química en la Facultad de Química de la Universidad Nacional Autónoma de México y una estancia posdoctoral en el Instituto Max Planck de Investigaciones sobre el Estado Sólido, en Stuttgart, Alemania. Es profesor de la Facultad de Química de la UNAM desde 1974 y Jefe de la División de Estudios de Posgrado. Actualmente, es presidente de la Sociedad Internet

de México, vicepresidente del Consejo Directivo de la Internet Corporation for Assigned Names and Numbers y miembro del Consejo Directivo de la Corporación Universitaria para el Desarrollo de Internet.

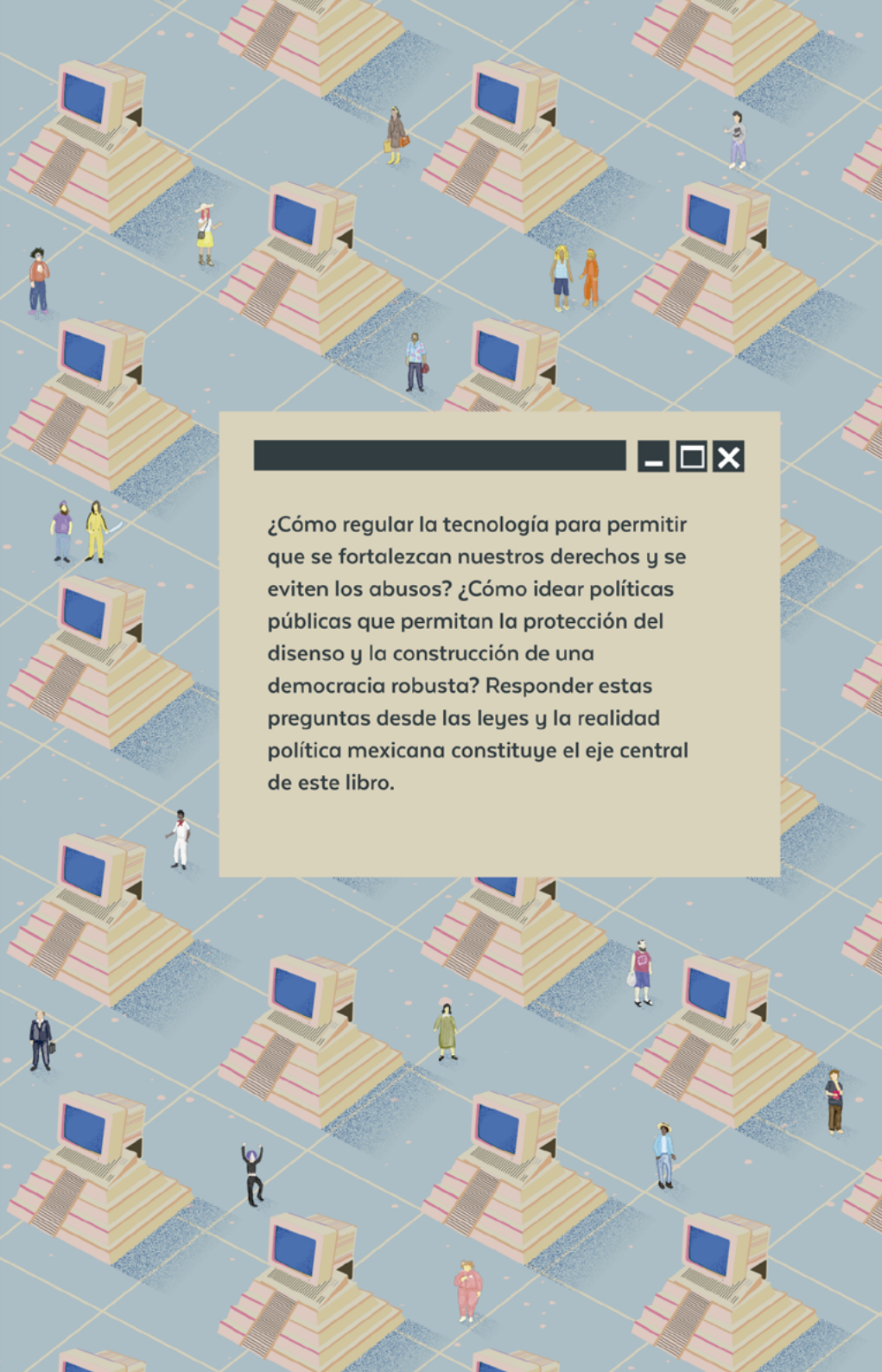
Erik Huesca Morales. Se formó como físico en la Facultad de Ciencias de la Universidad Nacional Autónoma de México y tiene maestría y doctorado en inteligencia artificial por la Universidad de California en Berkeley. Es presidente de la Academia Mexicana Informática, e introductor de internet en México y varios países de América Latina. En 2015 recibió el reconocimiento del HITEC como uno de los 50 latinoamericanos más influyentes de la industria, y es fundador del capítulo mexicano de Sociedad de Internet.

Paradojas del "gobierno abierto" en el contexto mexicano

Juan Manuel Casanueva. Es maestro en ciencias de Gestión e Implantación de Proyectos de Desarrollo por la Universidad de Manchester. Fundador de la ONG SocialTIC, dedicada al habilitamiento de actores de cambio a través del uso de la tecnología y la información. Ha coimpulsado los procesos de Gobierno Abierto (AGA) y Parlamento Abierto en México, así como las comunidades Escuela de Datos y Desarrollando América Latina.

Notas

Notas



¿Cómo regular la tecnología para permitir que se fortalezcan nuestros derechos y se eviten los abusos? ¿Cómo idear políticas públicas que permitan la protección del disenso y la construcción de una democracia robusta? Responder estas preguntas desde las leyes y la realidad política mexicana constituye el eje central de este libro.