LEGALIDAD DEL PROYECTO TOR: LA HERRAMIENTA DEL SIGLO XXI QUE GARANTIZA LA PRIVACIDAD Y SU USO EN MÉXICO

ALFREDO REYES KRAFFT

DERECHOS DIGITALES
América Latina

LEGALIDAD DEL PROYECTO TOR: LA HERRAMIENTA DEL SIGLO XXI QUE GARANTIZA LA PRIVACIDAD Y SU USO EN MÉXICO

ALFREDO REYES KRAFFT

DERECHOS DIGITALES
América Latina

Portada y diagramación: Javiera Méndez
Correcciones por Sebastian Alburquerque
Noviembre de 2018.

Esta publicación fue posible gracias al apoyo de Open Technology Fund

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción de la libertad de expresión, el acceso a la cultura y la privacidad.

Contenido

Legalidad del proyecto tor: la herramienta del siglo xxi que garantiza la privacidad y su uso en México

Actualmente, los avances tecnológicos en materia de comunicación nos permiten acortar las distancias y conectarnos de formas sencillas y eficaces con cualquier persona alrededor del mundo. Esto implica una ventaja excepcional con relación a la vida de las personas en el pasado, pero también conlleva un riesgo derivado del intercambio instantáneo de información de un punto a otro de nuestro planeta: de un clic a otro existe la posibilidad de que seamos identificados, y en consecuencia, sean vulnerados nuestros datos personales e incluso puedan ser mal utilizados para la comisión de ilícitos.

En este contexto, se ha desarrollado una herramienta tecnológica conocida como el Proyecto TOR. Es un software libre que permite a miles de usuarios su uso de forma anónima, lo cual abre la posibilidad de ejercer nuestro derecho a la libertad de expresión de forma privada, confidencial y abierta. Al respecto, nos surgen las siguientes interrogantes: ¿Conocemos de forma total y expresa los beneficios y riesgos que esto implica? ¿Sabemos las consecuencias legales que conlleva el uso de este tipo de plataformas en nuestro país?

The Onion Router, TOR, por su siglas en inglés, tiene como objetivo principal el realizar operaciones en la red de comunicaciones a baja latencia y de forma sobrepuesta en Internet, lo que permite que la información intercambiada por sus usuarios se realice de forma segura, íntegra y secreta, cuidando que no se revelen las identidades de estos. En otras palabras, el viaje que realiza la información dentro del Proyecto TOR se hace de forma que los datos cifrados circulan en forma de capas, como las de una cebolla, que a pesar de ser pelada no pierde sabor ni consistencia.

Para entender la experiencia que ofrece el Proyecto TOR, es necesario conocer las implicaciones legales que lo comprenden.

Los básicos de TOR

¿Qué es?

TOR es tanto un software libre como una red de conexión a Internet, que permite guardar el anonimato y privacidad al navegar en la red. Su finalidad es evitar la vigilancia que cualquier persona, empresa o gobierno pudiera ejercer sobre las personas. Esto se logra haciendo pasar los datos a través de tres servidores, los cuales forman parte de una red mundial de personas que donan su infraestructura y su ancho de banda para que esto sea posible. A dichos servidores se les conoce como nodos y se dividen conforme a su función en nodos de entrada, intermedios y de salida.

Clasificación de los Nodos[1]

Nodo de entrada. Es el servidor al que la computadora del usuario se conecta primero para comenzar a navegar por Internet, el cual envía los datos al siguiente nodo.

Nodo intermedio. Es un servidor de paso que permite conectar el nodo de entrada y de salida al tiempo que desvía el tráfico para evitar identificar a la persona usuaria.

Nodo de salida. Es el servidor que recibe los datos del nodo intermedio y conecta con la página de Internet que fue solicitada.

Con esto, los datos pasan por una ruta que es más difícil detectar lo que permite evadir el rastreo y la vigilancia.

TOR y sus usuarios

Esta herramienta tecnológica es utilizada por millones de usuarios diariamente, destacando principalmente los siguientes:

1. Personas comunes y corrientes que no desean ser rastreadas y vigiladas por las grandes compañías de Internet.
2. Denunciantes de corrupción que necesitan medios de comunicación seguros.
3. Víctimas de abuso y de acosadores que necesitan proteger su identidad.
4. Periodistas, activistas y disidentes políticos que sufren de monitoreo de sus actividades en línea.
5. Personas viviendo en Estados que restringen el acceso a Internet y/o vigilan a sus habitantes.

---

1 Tor Browser es un navegador anónimo diseñado para proteger su identidad y ubicación mientras navega por la web. En lugar de conectarte directamente con el sitio web que deseas visitar, Tor te hará brincar por una red de computadoras voluntarias (llamadas “nodos”) en tu camino hacia tu destino final. Esta rebotando alrededor de las máscaras, quién eres y de dónde te estás conectando. Esto hace que sea más difícil para las personas que lo monitorean saber lo que está haciendo en línea, y es más difícil para las personas que monitorean ciertos sitios saber quién los está usando y de dónde se están conectando.

Lo cual nos permite advertir claramente las ventajas que implica el uso de este sistema[2]. Sin embargo, existe una pequeña fracción de individuos que hacen mal uso de la red, ya sea para realizar ataques informáticos u otro tipo de abusos en línea, y aunque se han aplicado a este nodo medidas para disminuir este tipo de situaciones, no se han logrado erradicar en su totalidad. Esto ha alimentado los argumentos en su contra por parte de sus detractores.

Responsabilidad de uso de TOR

En esta plataforma, la responsabilidad de los sitios finales visitados corresponde únicamente a los usuarios de Internet. Como parte del proceso para otorgar anonimato, este nodo no conserva ninguna clase de registro sobre las páginas visitadas, medios de conexión, paquetes de datos que cruzan por él ni ningún dato que pueda identificar a las personas que lo utilizan. Solo se conservan datos estadísticos para fines de investigación.

Esto convierte a TOR en una herramienta sumamente poderosa para el envío de mensajes e intercambio de información a través de Internet, y que bien encausada se puede convertir en un canal de comunicación para los usuarios que por diversas circunstancias vean comprometida su integridad física o seguridad por la sola manifestación de sus ideas, es decir, que tienen coartados de alguna manera sus derechos humanos.

TOR y la libertad de expresión

El derecho a la libertad de expresión no sólo es un Derecho Humano reconocido internacionalmente en la Declaración Universal de los Derechos Humanos de 1948, que en su artículo 12 establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o a su reputación. Es también un derecho consagrado en diversos pactos y tratados internacionales.

En el Pacto Internacional de Derechos Civiles y Políticos de 1966, en su artículo 17, establece las mismas disposiciones que el artículo 12 de la Declaración Universal de los Derechos Humanos. En su artículo 19 al hablar de la libertad de expresión señala que el ejercicio de ese derecho entraña deberes y responsabilidades especiales por lo que podrá estar sujeto a ciertas restricciones fijadas por la ley y que sean necesarias para asegurar el respeto a los derechos o a la reputación de los demás, así como para proteger la seguridad nacional, el orden público, la salud o moral públicas.

En la Convención Americana Sobre Derechos Humanos de 1969, mejor conocida como Pacto De San José, en el artículo 11 se refiere a que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad y que por tanto no deberá ser objeto de injerencias arbitrarias o abusivas en su vida privada, familia, domicilio, correspondencia, ni deberá sufrir ataques ilegales a su honra o reputación. Y establece también el derecho de la persona a ser protegida por la ley contra esas injerencias o ataques.

---

2 Es importante recordar que Tor protegerá su privacidad y anonimato solo para actividades dentro de Tor. Tener instalado Tor en su computadora no hace que otras cosas que haga en su dispositivo, como la navegación web en otro navegador como Chrome o Firefox, sean más privadas o anónimas. Tampoco oculta el hecho de que estás usando Tor. Su navegación web puede ser anónima, pero quedará claro que está utilizando el software Tor. Tor tampoco encripta tu tráfico web; para eso necesitarás HTTPS. Es por eso que es clave visitar sitios web que admitan HTTPS dentro de Tor, de manera que los dos puedan trabajar juntos para brindarle seguridad y anonimato mientras navega.

El artículo 13 establece la libertad de pensamiento y expresión determinando que no deberá existir previa censura, pero que el ejercicio de esos derechos estará sujeto a responsabilidades ulteriores, mismas que deberán estar expresamente fijadas por la ley y que deberán tender a asegurar entre otras cuestiones, el respeto a los derechos o a la reputación de los demás.

La Convención sobre los Derechos del Niño de 1989, en su artículo 16 menciona que ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o a su reputación; y que el niño tiene derecho también a la protección de la ley contra esas injerencias y ataques.

Y no sólo eso, sino que también es un derecho constitucional debidamente reconocido y garantizado en el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, que a la letra dice:

> "Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.
>
> *Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.*"

De lo que antecede, podemos advertir que el uso de la herramienta tecnológica de referencia puede llegar a traducirse en el libre ejercicio de uno de los derechos fundamentales de las personas, que no obstante haber sido reconocido ampliamente a nivel tanto internacional como nacional, es vulnerado con frecuencia. Por ello la importancia de conocerla, así como identificar el impacto legal que tiene en nuestro país.

TOR y la Privacidad de Datos en México

Para delinear el impacto legal que tiene el uso de TOR en México, consideramos oportuno remitirnos al marco legal relacionado con la privacidad de datos personales.

Desde el año 2010, en la República Mexicana existe una legislación federal en materia de Protección de Datos Personales. En años anteriores existía únicamente regulación local en tres estados, a saber: Tlaxcala, Jalisco y Colima, la cual quedó sin efectos con la entrada en vigor de nuestra Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Asimismo, desde hace varias décadas existen disposiciones en diversas regulaciones que prevén la confidencialidad respecto de cierta información de carácter personal, por ejemplo, el secreto profesional y el secreto bancario, entre otros.

Fue en el año 2017 que en el ámbito público por fin se creó una normativa que estipula las obligaciones mínimas en la materia para los tres niveles de gobierno con la entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y con ella se dio inicio al efecto dominó que supone la obligación de cada uno de los Estados de la República para legislar en la materia.

Apenas en este año 2018, después de años de trabajo, cabildeo y reuniones de las autoridades de protección de datos personales, México logra su adhesión al Convenio 108 del Consejo de Europa, reafirmando su compromiso con la protección de los datos personales y de la privacidad.

TOR: el anonimato y el seudónimo en México

El anonimato y el seudónimo son dos conceptos abordados por la Ley Federal del Derecho de Autor en México. Constitucionalmente los derechos de autor y el derecho a la información están íntimamente ligados, así como el derecho a la privacidad y a la protección de los datos personales. En materia de derechos de autor, el autor goza de la prerrogativa de mantener en secreto su identidad para no ser víctima de censura o de persecución.

En términos del artículo 4º del ordenamiento legal en cita, una obra puede ser anónima o seudónima. En el primer caso, porque el autor publica o divulga su obra sin firmarla, ya sea por voluntad propia o por circunstancia. En el segundo caso, el autor hace pública su obra utilizando un seudónimo para no revelar su verdadera identidad. ya sea para garantizar su libertad de expresión, o bien, en casos más extremos, para proteger su integridad física y su vida.

En otros países la situación es completamente distinta. En Venezuela y Brasil el anonimato se encuentra expresamente prohibido en su Constitución. En Vietnam el uso de seudónimos es ilegal. En Rusia, se necesita registrarse para operar un blog, e incluso es obligatorio el registro de las tarjetas SIM; el número celular para utilizar el Internet público. En México no existe una prohibición legal del anonimato; incluso, la explotación de datos anonimizados se encuentra exceptuada de la aplicación de la LFPDPPP.

A este proceso de volver anónima la información de carácter personal se le conoce como disociación, la cual se encuentra definida en el artículo 3º de la LFPDPPP, como el procedi-

miento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Con lo anterior, se abre legalmente la posibilidad de la explotación de la información que ha sido disociada para diversos fines: desde los más básicos como estadística, hasta los más modernos y sofisticados como *open data, machine learning, data science, big data,* etcétera.

Sin embargo, el anonimato presenta algunos problemas prácticos ya que, si bien es cierto que por un lado sirve para garantizar derechos humanos básicos como la libertad de expresión o la seguridad personal a favor de sus usuarios, por otro lado también puede ser utilizado como herramienta para cometer actos ilícitos pretendiendo enmascarar la verdadera identidad del sujeto activo.

Sobre el particular, contrario a lo que supone el usuario promedio de Internet, la estructura y regulación actual de las telecomunicaciones en México, así como del marco regulatorio de los prestadores de servicios de Internet, permiten con relativa facilidad identificar no sólo a los usuarios, sino monitorear su actividad e incluso, llevar un récord de sus accesos a Internet.

Al respecto, encontramos que en términos del Título Octavo de la Ley Federal de Telecomunicaciones y Radiodifusión. De la Colaboración con la Justicia: los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes.

Por lo tanto, los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán, entre otras cosas, conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión, al menos los siguientes datos:

a. Nombre, denominación o razón social y domicilio del suscriptor;

b. Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

c. Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

d. Datos necesarios para determinar la fecha, hora y duración de la comunicación, asícomo el servicio de mensajería o multimedia;

e. Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

f. En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g. La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

h. La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

No hay que perder de vista que el deber de conservación del concesionario es sobre los datos de conexión. Al revisar el listado con suficiente atención, podemos advertir que no hay referencia sobre al contenido de la comunicación.

Para cumplir con la obligación legal descrita, el concesionario deberá conservar los datos enlistados durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

No obstante, cabe aclarar que en el Título Noveno. De los Derechos de los Usuarios y sus Mecanismo de Protección, se garantiza la protección a los datos personales de los mismos, por lo que el derecho a la privacidad y el de la protección de datos personales, únicamente podrán verse disminuidos en caso de que exista un mandamiento de autoridad debidamente fundado y motivado, en relación con algún asunto de seguridad.

Con lo que antecede, se hace patente la disposición Constitucional contemplada en el artículo 16 primero y segundo párrafos que al efecto establece:

> *"Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.*
>
> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."*

Es decir, aun cuando no existe ninguna prohibición respecto del anonimato y del uso de seudónimos en nuestro país, técnicamente hablando y para efectos prácticos, no sólo es viable la identificación de los usuarios, sino que es obligación legal de los proveedores de servicios de Internet y análogos contar con mecanismos de rastreo, identificación y conservación de datos personales.

Por tanto, resulta de particular trascendencia para el tema que nos ocupa, no perder de vista que el concesionario cumple con la obligación legal que se ha descrito al llevar a cabo la conservación de los referidos datos de conexión a la red TOR del usuario, pero dicho lineamiento no se extiende al contenido que ahí se encuentra anonimizado, pues la red TOR sólo funge como un intermediario de acceso.

El uso de herramientas de cifrado no está expresamente prohibido por la Ley, salvo cuando

este cifrado se lleva a cabo con fines ilícitos, por ejemplo: en los ataques de *ransomware* cuyo objetivo final es la extorsión de los usuarios para que entreguen algún tipo de contraprestación a cambio de las claves de descifrado de su información.

El cifrado, en nuestro país, está reconocido como una alternativa o herramienta para garantizar la seguridad y la confidencialidad de la información, por lo cual no está prohibido implementar este tipo de medidas siempre y cuando se utilicen con el consentimiento de los titulares de la información o de los medios de almacenamiento que correspondan.

El Acuerdo por el que se reforma y adiciona el diverso por el que se establecen las disposiciones administrativas en materia de tecnologías de la información y comunicaciones y de seguridad de la información, y se expide el Manual Administrativo de Aplicación General en esas materias, publicado el 22 de agosto de 2012, estipula expresamente que: "*se utilizarán mecanismos de cifrado de llave pública y privada, canales cifrados de comunicación y, cuando corresponda, de firma electrónica avanzada, que permitan la diseminación de la información únicamente al destinatario autorizado al que esté dirigida*."

TOR y los Proveedores de Servicios de Acceso a Internet

En México no existe una norma que prohíba la utilización de redes privadas virtuales (VPN) o servidores proxy, por lo tanto, no se pueden fincar responsabilidades legales a intermediarios que promuevan o faciliten el uso de estas herramientas; la criminalización o pena, debe ser de la conducta, no de la tecnología. Por lo tanto, si un usuario de una VPN o de un proxy cometiera algún ilícito de cualquier naturaleza, deberá ser sancionado por la conducta llevada a cabo independientemente de los medios que haya utilizado. Al menos en México, el simple uso de estas herramientas no constituye en sí mismo una conducta ilícita.

Hoy en día, la legislación mexicana no prevé la corresponsabilidad para los proveedores de servicios de acceso a Internet, por las violaciones en materia de propiedad intelectual cometidas a través de sus servicios o herramientas digitales, siempre y cuando no exista conocimiento, dolo o apología del delito. Es decir, que se promueva la herramienta como instrumento idóneo para la comisión de un delito.

Como ejemplo de lo anterior, tenemos el caso de las plataformas de almacenamiento en la nube. Si éstas se promovieran como un medio para almacenar contenido ilícito o se beneficiaran de éste, sin duda alguna serían corresponsables; pero si el usuario, a pesar de ser advertido de las faltas en las que podría incurrir y sus respectivas sanciones en caso de violar derechos de propiedad intelectual lleva a cabo estas conductas, el intermediario no tiene por qué ser sancionado.

Una alternativa que se ha puesto en marcha en sitios mexicanos, sobre todo de *market places,* es la de abrir canales de comunicación con usuarios que puedan denunciar cuando advierten que sus derechos de propiedad intelectual son objeto de violación por parte de un tercero y en consecuencia, los contenidos son retirados oportunamente del sitio con lo cual garantizan que actúan de buena fe en su calidad de intermediarios.

En este sentido, los artículos 145 y 146 la Ley Federal de Telecomunicaciones y Radiodifusión, establecen a favor de los usuarios de los servicios de acceso a Internet las siguientes prerrogativas:

"Artículo 145. Los concesionarios y autorizados que presten el servicio de acceso a Internet deberán sujetarse a los lineamientos de carácter general que al efecto expida el Instituto conforme a lo siguiente:

I. Libre elección. Los usuarios de los servicios de acceso a Internet podrán acceder a cualquier contenido, aplicación o servicio ofrecido por los concesionarios o por los autorizados a comercializar, dentro del marco legal aplicable, sin limitar, degradar, restringir o discriminar el acceso a los mismos.

No podrán limitar el derecho de los usuarios del servicio de acceso a Internet a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos que se conecten a su red, siempre y cuando éstos se encuentren homologados;

II. No discriminación. Los concesionarios y los autorizados a comercializar que presten el servicio de acceso a Internet se abstendrán de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicio;

III. Privacidad. Deberán preservar la privacidad de los usuarios y la seguridad de la red;

IV. Transparencia e información. Deberán publicar en su página de Internet la información relativa a las características del servicio ofrecido, incluyendo las políticas de gestión de tráfico y administración de red autorizada por el Instituto, velocidad, calidad, la naturaleza y garantía del servicio;

V. Gestión de tráfico. Los concesionarios y autorizados podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red conforme a las políticas autorizadas por el Instituto, a fin de garantizar la calidad o la velocidad de servicio contratada por el usuario, siempre que ello no constituya una práctica contraria a la sana competencia y libre concurrencia;

VI. Calidad. Deberán preservar los niveles mínimos de calidad que al efecto se establezcan en los lineamientos respectivos, y

VII. Desarrollo sostenido de la infraestructura. En los lineamientos respectivos el Instituto deberá fomentar el crecimiento sostenido de la infraestructura de telecomunicaciones.

Artículo 146. Los concesionarios y los autorizados deberán prestar el servicio de acceso a Internet respetando la capacidad, velocidad y calidad contratada por el usuario, con independencia del contenido, origen, destino, terminal o aplicación, así como de los servicios que se provean a través de Internet, en cumplimiento de lo señalado en el artículo anterior."

En estos artículos se establece el principio de neutralidad tecnológica; por lo que ningún proveedor de servicios de acceso a Internet está facultado para bloquear el acceso a ninguna red, incluido el Proyecto TOR, pues al hacerlo estaría dañando de forma directa la capa de confidencialidad favorable que esta red le proporciona a sus usuarios.

TOR y la Policía Federal

La Policía Federal es un órgano administrativo descentralizado de la Secretaría de Seguridad Pública, y dentro de sus objetivos se encuentra la salvaguarda de los derechos de las perso-

nas, así como preservar las libertades, el orden y la paz públicos. Cuenta con diversas Unidades Adminsitrativas encargadas de la investigación y ofrece servicios técnicos especializados que la Dependencia requiera.

La División Científica se encarga de generar metodología científica y tecnológica para la prevención e investigación del delito, a través del desarrollo de herramientas técnico-científicas, con la participación de personal experto en criminalística, investigación cibernética y seguridad de sistemas de información y servicios científico-tecnológicos, que contribuyen a los objetivos de la Policía Federal.

Esta División cuenta con veinte atribuciones, plenamente establecidas en el artículo 15 del Reglamento de la Ley de la Policía Federal, que a la letra establece:

"Artículo 15.- Corresponde a la División Científica:

I. Utilizar los conocimientos y herramientas científicas y técnicas en la investigación para la prevención de los delitos;

II. Coordinar, supervisar y operar el funcionamiento de los servicios científicos y técnicos de la Institución;

III. Auxiliar a las unidades de la Institución y a las autoridades competentes que lo soliciten, en la búsqueda, preservación y obtención de indicios y medios de pruebas necesarios en la investigación de delitos;

IV. Identificar y preservar, en el ámbito de su competencia y conforme a las disposiciones aplicables, la integridad de los indicios, huellas o vestigios del hecho delictuoso, así como los instrumentos, objetos o productos del delito;

V. Preservar el lugar del hecho delictuoso, fijar, señalar, levantar, embalar y entregar la evidencia física a las autoridades competentes, conforme al procedimiento previamente establecido por éstas y en términos de las disposiciones aplicables;

VI. Proporcionar la información que requieran las autoridades competentes, a fin de apoyar el cumplimiento de las funciones constitucionales de investigación para la prevención y combate de los delitos;

VII. Vigilar, en el ámbito de su competencia, el cumplimiento de los lineamientos de la cadena de custodia, con la finalidad de preservar la integridad de los indicios, evidencias y pruebas;

VIII. Establecer los lineamientos internos que deban observarse, para la emisión de opiniones conforme a la normatividad de la materia;

IX. Dictar las políticas y procedimientos institucionales para la actuación de los servicios de apoyo técnico-científico;

X. Coordinar el funcionamiento de los laboratorios criminalísticos de la Institución, cuyo objeto es analizar los elementos químicos, biológicos, tecnológicos y mecánicos, que apoyen la investigación para la prevención de delitos y en el esclarecimiento de hechos delictuosos bajo la conducción y mando del Ministerio Público;

XI. Supervisar la actualización de las bases de datos criminalísticos y de personal de la Institución, con datos de utilidad en la investigación de delitos, sin afectar el derecho de las personas sobre sus datos personales;

XII. Establecer los mecanismos para la participación y comunicación con organismos y autoridades nacionales e internacionales, relacionados con las atribuciones de su competencia;

XIII. Incorporar huellas dactilares, fotografías, videos y otros elementos que sirvan para identificar a una persona, a las bases de datos de la Institución y de la Secretaría, en términos de las fracciones XVII y XXV del artículo 8 de la Ley;

XIV. Supervisar que las opiniones cumplan con las formalidades científicas y técnicas aplicables y acaten la normativa vigente;

XV. Proponer al Comisionado General, la intervención de comunicaciones y operaciones encubiertas, en coordinación con la División de Inteligencia;

XVI. Vigilar, identificar, monitorear y rastrear la red pública de Internet, para prevenir conductas delictivas;

XVII. Establecer registros de la información obtenida con motivo de sus investigaciones, así como instituir mecanismos y protocolos para garantizar la confidencialidad e integridad de los datos;

XVIII. Implementar los mecanismos que impulsen la investigación científica en áreas de oportunidad que deriven en metodologías y herramientas para la modernización continua de las diversas áreas de la Institución;

XIX. Participar, en coordinación con la División de Inteligencia, en las operaciones encubiertas y de usuarios simulados, y

XX. Las demás que le confieran este Reglamento, otras disposiciones legales aplicables o aquéllas que le encomiende el inmediato superior de quien dependa."

En este sentido, es posible advertir que resulta completamente legal en nuestro país el monitoreo de Internet por parte de la Policía Federal para la prevención de ilícitos, y en casos donde exista una denuncia presentada ante el Ministerio Público o cualquier otra autoridad, la Policía Federal podrá colaborar en la investigación de la probable comisión de un delito.

Esta División es la encargada de instrumentar, operar y resguardar las bases de datos de la Policía Federal para la adopción de estrategias en materia de seguridad pública; realiza las acciones necesarias para garantizar el suministro, intercambio, sistematización, consulta, análisis y actualización de la información que a diario se genera sobre seguridad pública para la toma de decisiones del Gobierno Federal.

Por lo tanto, será esta autoridad la competente en México para llevar a cabo la investigación correspondiente a fin de determinar si existen elementos suficientes para afirmar que una herramienta tecnológica, como es el caso de TOR, es utilizada por un usuario de Internet con fines ilícitos y en su caso, la que podrá coadyuvar a las autoridades judiciales para la imposición de las sanciones correspondientes.

TOR como evidencia y su valor probatorio a nivel judicial

Un sistema probatorio es el conjunto de normas conforme a las cuales se regulan las pruebas en el enjuiciamiento y su forma de evaluarlas, es decir, a través de cada sistema probatorio, podremos saber cuáles pruebas pueden llevarse al proceso y qué valor demostrativo repre-

sentan. En México contamos con un sistema libre y una lógica de valoración de la prueba que forman parte del sistema penal acusatorio.

Es decir, que para acreditar la comisión de un delito puede presentarse cualquier elemento digital como prueba, ya que este modelo presupone conferir libertad al juzgador de apreciar el elemento de convicción y otorgarle, bajo un proceso racional, un determinado valor. Sin embargo, si bien se trata de una inicial libertad para efectuar tal operación mental, el juzgador debe basarse en reglas del raciocinio para llegar a su conclusión, así como apoyarse en la experiencia y la ciencia. De esa manera, tenemos un sistema de valoración libre racional.

En efecto, el Constituyente permanente y el legislador, al crear el sistema penal acusatorio mexicano, establecieron de manera clara que la prueba debe valorarse de manera libre y lógica, tal como se advierte del artículo 20, apartado A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, al preceptuar:

> *"Artículo 20. El proceso penal será acusatorio y oral. Se regirá por los principios de publicidad, contradicción, concentración, continuidad e inmediación.*
>
> *A. De los principios generales:*
>
> *(...)*
>
> *II. Toda audiencia se desarrollará en presencia del juez, sin que pueda delegar en ninguna persona el desahogo y la valoración de las pruebas, la cual deberá realizarse de manera libre y lógica..."*

Así como de los diversos 259, párrafo segundo, 265 y 402, del Código Nacional de Procedimientos Penales, que a la letra indica:

> "Artículo 259. Generalidades.
>
> *Cualquier hecho puede ser probado por cualquier medio, siempre y cuando sea lícito.*
>
> *Las pruebas serán valoradas por el órgano jurisdiccional de manera libre y lógica.*
>
> *(…)*
>
> *Artículo 265. Valoración de los datos y prueba.*
>
> *El órgano jurisdiccional asignará libremente el valor correspondiente a cada uno de los datos y pruebas, de manera libre y lógica, debiendo justificar adecuadamente el valor otorgado a las pruebas y explicará y justificará su valoración con base en la apreciación conjunta, integral y armónica de todos los elementos probatorios.*
>
> *(..)*
>
> *Artículo 402. Convicción del Tribunal de enjuiciamiento.*
>
> *El Tribunal de enjuiciamiento apreciará la prueba según su libre convicción extraída de la totalidad del debate, de manera libre y lógica; sólo serán valorables y sometidos a la crítica racional, los medios de prueba obtenidos lícitamente e incorporados al debate conforme a las disposiciones de este Código*."

En mérito de lo anterior, el sistema de valoración de la prueba presupone dos supuestos:

a. Una libertad valorativa de la prueba.

b. Una lógica que conlleva a una natural motivación de las decisiones del órgano jurisdiccional.

De manera genérica, siempre y cuando las evidencias se hayan obtenido de forma lícita y estén intrínsecamente relacionadas con la conducta que pretende probarse, se pueden presentar sin ningún problema. Entendamos que por la naturaleza de TOR existe un cierto grado de anonimato de los usuarios, sus conexiones y sus equipos, no así de algún tipo de datos que compartan de manera voluntaria con otros usuarios y que en conjunto con otros datos de investigación pudieran ser vinculados para generar convicción en el juzgador como medio de prueba.

Es poco probable que un ToR Relay pudiera ser incautado si tomamos en cuenta de que el medio no está intrínsecamente ligado a la conducta, sin embargo, si en el curso de la investigación pudiese comprobarse que una red delictiva es titular de un Relay, éste pudiera ser incautado, como en cualquier otro caso y bajo las mismas reglas procedimentales. Es decir. en total y completo apego al debido proceso y previo mandamiento de autoridad judicial.

Para entender un poco más sobre la valoración de pruebas obtenidas por medios electrónicos, podemos remitirnos al contenido del artículo 210-A del Código Federal de Procedimientos Civiles donde se establece de forma expresa el reconocimiento como prueba de toda la información generada o comunicada que conste en medios electrónicos, considerándola mayormente fiable si es posible conocer el método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. El juez deberá de apoyarse, en caso de ser necesario, por peritos en la materia que ayuden a reforzar la valoración de las mismas.

A mayor abundamiento, el mismo dispositivo legal establece que cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada en medios electrónicos, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta. Sobre el particular, se han pronunciado nuestros más altos tribunales en los siguientes términos:

> *"Registro No. 178929 Localización:*
> *Novena Época Instancia: Tribunales Colegiados de Circuito*
> *Fuente: Semanario Judicial de la Federación y su Gaceta XXI, Marzo de 2005*
> *Página: 1205*
> *Tesis: II.1o.A.21 K*
> *Tesis Aislada Materia(s): Común*
>
> *PRUEBAS EN EL AMPARO. PARA EL DESAHOGO DE LAS RELACIONADAS CON MEDIOS ELÉCTRICOS O ELECTRÓNICOS NO ES ADMISIBLE LA IMPOSICIÓN DE CARGA ESPECÍFICA A SU OFERENTE PARA VALORAR SU ADMISIBILIDAD.*
>
> *Además de los medios clásicos o tradicionales de prueba, la rápida evolución de la técnica ha creado nuevos métodos probatorios antaño in sospechados que, en parte, debido a su constante innovación y dadas las particularidades que cada uno de ellos pueden*

presentar, no han sido regulados en detalle por el legislador, pero la posibilidad de aportarlos como elementos de convicción está prevista tanto en el artículo 150 de la Ley de Amparo como en los artículos 93, 188, 189, 210-A y 217 del Código Federal de Procedimientos Civiles supletorio de aquélla. En razón de ello, el juzgador deberá determinar en cada caso concreto y según sus propias características, la forma más conveniente para el desahogo y valoración de tales medios de convicción; sin embargo, el legislador en ningún caso previó que las peculiaridades de tales probanzas tuvieran como efecto imponer cargas específicas a los quejosos, como sería el caso de solicitar a éstos que aportaran algún tipo de aparato (como televisión o videocasetera), a fin de que se valorara la admisibilidad de su prueba, ya que no es posible tener la certeza de que los quejosos cuenten con la posibilidad real y material de aportar tales aparatos eléctricos o electrónicos, y dado que el juicio de garantías constituye una defensa del gobernado frente a actos arbitrarios de la autoridad, no resulta aceptable que su acceso se haga depender de la posibilidad de disponer de determinados bienes materiales. Por ello, se estima que la imposición a los quejosos de tal carga afecta el derecho a probar y, por ello, implica violación a las leyes del procedimiento. PRIMER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL SEGUNDO CIRCUITO. Amparo en revisión 480/2004. Sebastián Pallares Robles y otros. 25 de noviembre de 2004. Unanimidad de votos. Ponente: Salvador Mondragón Reyes. Secretaria: Sonia Rojas Castro."

En este orden de ideas, es claro que la información presentada como prueba en un juicio relacionada con TOR, se generó y almacenó de forma digital, por lo tanto, su valoración quedará sujeta al prudente arbitrio del juzgador, quien tendrá la obligación de allegarse de los elementos necesarios para otorgarle el valor probatorio correspondiente, sin que su simple uso pueda significar en sí mismo, la posible comisión de un ilícito.

¿Cuál es la importancia del Proyecto TOR?

Para entender la importancia del Proyecto TOR como una herramienta que facilita la forma en que ejercemos nuestros derechos fundamentales, es necesario tomar en cuenta algunos términos que nos permiten advertir los alcances y dimensiones jurídicas que implica su uso.

Uno de estos términos es la neutralidad en la red, definido como: "*las situaciones de hecho en que la información se genera, archiva o transmite en forma de comunicaciones electrónicas, independientemente de la tecnología o del medio que se haya utilizado*"[3].

Puesto en términos simples la neutralidad tecnológica es la obligación que tiene el proveedor de servicios de Internet de tratar todo el tráfico de datos de forma igual sin cobrar tarifas extra por el contenido o la tecnología que el usuario decida utilizar. Es tratar a todas las páginas por igual sin que la forma en que sean consultadas afecte de alguna manera la prestación del servicio.

El Proyecto TOR, es "*una red abierta que le permite a los usuarios defenderse contra el análisis de tráfico que realizan algunas instancias gubernamentales sobre Internet, y que es una forma de vigilancia que amenaza la libertad personal, la privacidad, la confidencialidad en los negocios,*

3 Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales. Recuperado de : http://www.wipo.int/edocs/lexdocs/treaties/es/uncitral-uecic/trt_uncitral_uecic.pdf

así como las relaciones y la seguridad del Estado"[4]. Jurídicamente, el Proyecto TOR es importante por una simple razón: permite ejercer los derechos fundamentales de sus usuarios.

En conclusión, consideramos que TOR garantiza la privacidad y anonimato de las personas que ejercen su derecho a la libertad de expresión, pues mediante su red de múltiples capas de encriptación, mantiene la información sobre la ruta que se propagará el mensaje hasta encontrar el equipo "embudo de salida", que entregará la información al usuario final de una forma segura, integra y secreta, cuidando que no se revelen las identidades del emisor ni del receptor. Este sólo hecho no viola de manera alguna las disposiciones legales vigentes en México, por lo tanto, su uso constituye una alternativa jurídicamente viable para el intercambio de información a través de Internet de una manera más confiable.

4 What is Tor?. Recuperado de https://www.torproject.org/index.html

Referencias:

Declaración Universal de los Derechos Humanos, 1948. Recuperado de: http://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf

Pacto Internacional de los Derechos Civiles y Políticos, 16 de diciembre de 1966. Recuperado de: https://www.colmex.mx/assets/pdfs/2-PIDCP_49.pdf?1493133879

Convención Americana sobre Derechos Humanos , 22 de noviembre de 1969. Recuperado de: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales. Recuperado de: http://www.wipo.int/edocs/lexdocs/treaties/es/uncitral-uecic/trt_uncitral_uecic.pdf

Constitución Política de lo Estados Unidos Mexicanos, Diario Oficial de la Federación, Publicado: 5 de febrero de 1917, última reforma: 15 de septiembre de 2017.

Código Federal de Procedimientos Civiles, Diario Oficial de la Federación: 24 de febrero de 1943, última reforma: 09 de abril de 2012.

Código Nacional de Procedimientos Penales, Diario Oficial de la Federación: 05 de de marzo de 2014, última reforma: 17 de junio de 2016.

Ley Federal del Derecho de Autor, Diario Oficial de la Federación: 24 de diciembre de 1996, última reforma: 13 de enero de 2016.

Ley de la Policía Federal, Diario Oficial de la Federación, 01 de junio de 2009, última reforma: 15 de mayo de 2011.

Reglamento de la Ley de la Policía Federal, Diario Oficial de la Federación, 17 de mayo de 2010, última reforma: 22 de agosto de 2014.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Diario Oficial de la Federación: 05 de julio de 2010.

Ley Federal de Telecomunicaciones y Radiodifusión, Diario Oficial de la Federación:14 de julio de 2014, última reforma: 15 de junio de 2018.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Diario Oficial de la Federación: 26 de enero de 2017.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina