CAPÍTULO XV

METADATOS VS PRIVACIDAD: LA INSOPORTABLE LEVEDAD DE LA RED

Dr. Diego Alfredo Pérez Rivas
Universidad Autónoma de Baja California (FCAyS)

Actualmente vivimos en un periodo histórico en el que el almacenamiento de los metadatos de los usuarios de la red es una realidad imperante. Los planes de negocios de las redes sociales y los grandes buscadores concentran su atención en el almacenamiento de estos datos personales. Este tipo de empresas pueden describirse como memorias universales con la capacidad de registrar, procesar y administrar todo tipo de información mediante tecnologías asociadas al tratamiento de *big data*. El valor de mercado de las empresas está de hecho íntimamente asociado con la capacidad con la que cuentan para acumular información y usarla comercialmente.

Con la evolución de nuevos algoritmos inteligentes capaces de analizar gran cantidad de datos, como la que producen los usuarios en su interacción con los dispositivos digitales, se puede esperar el surgimiento de un nuevo mercado de los datos personales. El primer paso lo ha dado este año Donald Trump al revocar las reglas de *Protección de Datos de los Proveedores de Servicios de Internet* aprobadas durante la administración Obama por la *Federal Communications Commission* (FCC).[131] Todas estas condiciones han abierto un serio debate respecto al uso de los metadatos en el que se disputa la primacía de la privacidad de las personas, las reglas del libre mercado o la seguridad nacional.

Con la presente contribución se busca reflexionar acerca de las implicaciones éticas y jurídicas de dicha disputa en el caso mexicano. Esto se realizará a través del desarrollo de algunos aspectos esenciales. Primeramente resulta necesario contextualizar el escenario político en el que el debate surgió. En segundo lugar, es preciso conocer el estado del arte respecto al análisis de metadatos mediante nuevas tecnologías, así como conocer la normativa que regula el tratamiento de esta información en el contexto mexicano. Finalmente, mostrar los datos de asociaciones como la *Red en Defensa de los Derechos Digitales* nos ayudará a conocer el uso real de los datos de los usuarios para saber hasta qué punto puede constituir un peligro para el Estado de Derecho y la democracia.

131 Kang, Cecilia (2017) "Congress Moves to Strike Internet Privacy Rules From Obama Era", *The New York Times,* 23/03/2017. En: https://www.nytimes.com/2017/03/23/technology/congress-moves-to-strike-internet-privacy-rules-from-obama-era.html

1. Contexto

En abril de 2008 se realizó una de las primeras protestas organizadas a través de las redes sociales (*Facebook*) en el Cairo (Egipto) contra el gobierno de Mubarak. En breve diversos medios de comunicación informaron que los organizadores de la protesta fueron localizados por agentes públicos utilizando las bases de datos de la red social usada para la difusión.[132] Los administradores del grupo *Facebook* "movimiento 6 de abril" fueron sometidos a torturas. En 2011 uno de los manuales que sirvieron para organizar la revolución egipcia recomendaba que no se debía difundir esta información por *Twitter* o *Facebook*, advirtiendo sobre los potenciales riesgos para los disidentes. Muy pronto, Mubarak implementaría una política de censura y persecución en la red. [133]

Con el caso de Egipto se inició un debate que prosigue hasta nuestros días. Por una parte, las redes sociales jugaron un papel muy importante para la organización de las protestas y las manifestaciones civiles, fortaleciendo los mecanismos democráticos para la manifestación de las ideas y la libertad de asociación. El uso sincronizado de estas tecnologías posibilitó que personas de las más diversas procedencias pudieran ponerse de acuerdo y crear estrategias para combatir al mal gobierno y a la represión gubernamental. Por otro lado, el uso de esas mismas tecnologías para localizar a los ciudadanos participantes en las protestas, mostró hasta qué punto podría resultar peligroso que las autoridades estatales tuvieran acceso indiscriminado a la información generada en las redes. Las nuevas tecnologías se mostraron como un arma de doble filo, pues podían servir como un instrumento idóneo para la organización social y la democracia, pero también podían servir como una herramienta represiva en caso de que fueran usadas por gobiernos que no respetasen los derechos humanos. De este modo, en nombre de la *seguridad nacional* fue posible violentar la privacidad y los derechos civiles de los manifestantes.

En 2010, *WikiLeaks* reveló una serie de registros gubernamentales clasificados (*Collateral Murder, War Logs y Cablegate*) para denunciar los abusos sistemáticos del ejército y del gobierno de Estados Unidos en algunas operaciones militares.[134] Como respuesta, el gobierno de Obama orquestó una campaña jurídico-política para hacer callar a *WikiLeaks*. Para realizar la batalla jurídica se constituyó un gran jurado entre el Ministerio de la Justicia y el FBI, con el fin determinar si Assange podía ser incriminado por *complot* usando como referencia la *Espionage Act* de 1917. Entre

[132] Ver Farouk, Yasm ine (2012) "La revolución de Egipto: muy pronto para concluir, a tiempo para excluir", en *Foro Internacional*, El Colegio de México, núm. 2, pp. 345 y ss.
[133] Assange, Julian (2013) *Internet è il nemico*, Feltrinelli, Milano
[134] Bumiller, Elisabeth (2010) "Video Shows U.S. Killing of Reuters Employees", *The New York Times*, 05/04/2010. En http://www.nytimes.com/2010/04/06/world/middleeast/06baghdad.html

las estrategias que Assange ha denunciado en su contra se encuentran la exhortación a su asesinato, la censura directa, el bloqueo bancario, la persecución de sus asociados y el secuestro de equipos electrónicos.[135]

En este caso el dilema entre *seguridad nacional* y *transparencia* se resolvió en favor del *secreto de Estado* respecto a temas considerados como sensibles. Se trata evidentemente de una batalla ganada por la vigilancia, en el sentido de que surgiría en el imaginario colectivo un nuevo *enemigo público* cuyo delito parece consistir en hacer pública información que por alguna razón política debería considerarse como clasificada y peligrosa. Pero el verdadero escándalo estaba todavía por llegar.

Finalmente, en junio de 2013 los diarios *The Washington Post* y *The Guardian* publicaron una serie de documentos filtrados por Edward Snowden acerca de los programas de espionaje masivo de Estados Unidos y sus aliados a través de sistemas sofisticados como *Tempora, PRISM, XKeyscore*.[136] Al igual que con Assange, el otrora consultor tecnológico de la NSA sería acusado de espionaje al filtrar documentos considerados de *seguridad nacional*. Actualmente Snowden es un refugiado político en Rusia. En este caso específico, los documentos expusieron la faz más monstruosa de las políticas antiterrorismo puestas en marcha después de los acontecimientos del 11 de septiembre de 2001. En nombre de la *seguridad nacional*, la privacidad de millones de personas en todo el mundo ha sido violentada sistemáticamente mediante la puesta en marcha de sistemas informáticos capaces de gestionar grandes bases de datos para el espionaje. La justificación moral y política de estas acciones ha consistido en insistir que se trata de una lucha sin tregua contra el terrorismo. En otras palabras, la seguridad nacional que prima sobre la privacidad.

2. Metadatos

Los metadatos son un tipo de información muy especial que a nivel técnico sirven para organizar, clasificar y estructurar un conjunto de datos más numerosos y complejos. Un ejemplo intuitivo son las taxonomías que existen en las bibliotecas para organizar los inventarios. Los antiguos catálogos con fichas bibliográficas, o los más modernos sistemas digitales, contienen una gran cantidad de metadatos que ayudan a gestionar los datos primarios. En otras palabras, los metadatos son datos que hacen uso de una l*ógica de segundo orden*, un sistema abstracto basado en la información de *primer orden o datos fuente (los libros, capítulos, apartados, etc)*.

---

[135] Assange, *Op Cit*, pp. 21-28.

[136] Stöcker, C, y Lischka, K (2013) "New Leaks Show Near Total NSA Surveillance", *Spiegel online*, 01/08/2013. En: http://www.spiegel.de/international/world/new-nsa-leaks-describe-total-surveillance-system-xkeyscore-a-914244.html

En *Dublin Core Metadata Initiative FAQ* los metadatos son concebidos, por lo mismo, como "datos estructurados acerca de datos". Los metadatos son un tipo de datos que ayudan a los sistemas informáticos a clasificar y dar sentido a los recursos para clasificar la información. Una de sus funciones principales consiste en facilitar al usuario del sistema, sea una persona o un programa, el acceso a datos específicos sin la necesidad de consultar cada uno de los registros. En este sentido, se puede decir que los metadatos hacen posible que el sistema discrimine información dependiendo de las necesidades del usuario, creando también una propia sintaxis. Actualmente nosotros hacemos usos de estas tecnologías mediante diversos instrumentos en la red como por ejemplo cuando accedemos a algún buscador en línea o cuando buscamos algún artículo en *Wikipedia*.

Por otra parte, una definición funcional propone que los metadatos "son datos asociados con objetos que ayudan a los usuarios potenciales a tener conocimiento completo de sus características, entendiendo que el usuario puede ser un programa secundario o una persona".[137] Los metadatos son considerados como un instrumento informático imprescindible para la gestión y administración de las bases de datos. De hecho, están constituidos por información que estructura los recursos de los datos de primer orden, siendo susceptibles de ser ordenados a su vez en una lógica de tercer orden a través de *metadatos sobre metadatos* y así sucesivamente según el siguiente esquema:

Datos de primer orden →Metadatos (Datos de datos)→Metadatos de Metadatos→….∞

Esto evoca en cierto sentido la genial metáfora de la *Biblioteca de Babel* de Jorge Luis Borges. Esto es, un compendio de información que incluye datos sobre todos los datos posibles, como si se tratará de un juego de cajas chinas al infinito. Las principales funciones de los metadatos pueden ser sintetizadas de la siguiente manera:

1. Ubicación: sirven para encontrar particulares datos al interior de un archivo.
2. Búsqueda: datos que facilitan encontrar archivos específicos.
3. Gestión de recursos: ayuda a administrar los bancos de datos y catálogos, dotándolos de un lenguaje de segundo orden que posibilita su organización sistemática.

---

[137] Lorcan Dempsey and Stuart L.Weibel (1996) *The Warwick Metadata Workshop: A Framework for the Deployment of Resource Description. D-Lib Magazine*, July/August 1996. http://www.dlib.org/dlib/july96/07weibel.html . Y Lou Burnard et al (1996) *A Syntax for Dublin Core Metadata: Recommendations from the Second Metadata Workshop*. April 1996. http://www.uic.edu/~cmsmcq/tech/metadata.syntax.html

4. Interoperabilidad semántica: Ayuda a la estandarización de los archivos, facilitando la comunicación entre diferentes sistemas o plataformas.

El crecimiento exponencial en el potencial de almacenamiento de la información y la importante reducción de su costo económico han creado la necesidad de desarrollar instrumentos que ayuden en la gestión de las bases de datos. En este sentido, los *metadatos* y los *metadatos de metadatos* forman ya una realidad consolidada, esto es, una ontología y un lenguaje propio en el mundo de la informática y las comunicaciones digitales. El problema de todo esto surge cuando nos preguntamos qué tipo de metadatos poseen las empresas de telecomunicación o las grandes compañías del internet acerca de las personas y cuál es el posible uso que se le puede dar.

Actualmente estamos acostumbrados a la aparente gratuidad de los servicios digitales que ofrecen diversas compañías en internet. Las redes sociales, los buscadores, las agendas online, el servicio de correo electrónico, los videos consultados en la web, etc., tienen para el usuario un costo cero ¿Cómo es posible entonces que esas compañías hayan crecido exponencialmente si lo que hacen es ofrecer servicios que no son pagados por los usuarios? ¿Quién paga en realidad por todos estos servicios? El crecimiento exponencial de las compañías tiene que ver con el hecho de que son consideradas como imprescindibles minas de datos que almacenan un tesoro (la información) con valor comercial. Esto constituye en realidad el verdadero potencial de su valor de mercado.

La aparente gratuidad de los servicios digitales no facilita que el usuario reflexione acerca de lo que realmente está sucediendo con el servicio brindado por las empresas web y de telecomunicaciones. En realidad, en sus planes de negocios los datos y los metadatos son la mercancía que producen, mientras que el usuario se transforma de consumidor en producto. Este *giro copernicano* es posible gracias al almacenamiento y la gestión de los datos personales y de los metadatos en la red. Las empresas brindan los servicios a cambio de un acceso prácticamente completo a todos los datos proporcionados por el usuario. Se trata en realidad de un intercambio comercial entre los servicios de las empresas y la información personal de los usuarios.

Pero es importante preguntarnos por qué adquieren valor de mercados los metadatos. Para entender cómo es esto posible resulta necesario estar conscientes de que en nuestra interacción con las tecnologías digitales disponibles actualmente, generamos una especie de *huella digital* que puede servir para identificarnos analizando el uso de los dispositivos electrónicos desde los que accedemos a los servicios de la red. Los metadatos que los usuarios generan en su interacción con sus dispositivos y la red son el lenguaje en el que está escrita la huella digital.

La huella digital es una marca personal de los usuarios que se obtiene almacenando y analizando datos sobre los dispositivos que usan para la conectividad, los ip's, las interacciones de los usuarios entre sí o con otros sistemas, incluyendo fotos, mensajes escritos o de audio, correos electrónicos, compras, ubicación, datos relativos a las comunicaciones personales, agenda, datos biométricos, historial de búsquedas, los likes, datos recabados a través de cookies, etc. L*a insoportable levedad de la red* proviene del hecho de que los usuarios ceden casi todos esos datos voluntariamente, que no son otra cosa que rastros y patrones personales que pueden ser analizados, siendo apenas conscientes del modo en el que la entrega de esa información puede lesionar la privacidad e intimidad personal.

Una serie de preguntas son: ¿Cómo se gestiona toda esa información? ¿Sirve únicamente para "fines publicitarios legítimos" o su análisis bajo ciertas técnicas puede constituir una invasión a la privacidad y libertad personal? ¿La información proporcionada sirve únicamente para la explotación comercial de las empresas que las recogen o también son susceptibles de ser recolectadas y analizadas por agencias gubernamentales? ¿Surgirá en el futuro inmediato un mercado de la información en el que los datos sensibles puedan ser comercializados abiertamente o quizá en un mercado negro? ¿Qué tipo de reglas deben prevalecer?

Algunos estudios recientes han mostrado un posible sendero a seguir, haciendo patente la enorme potencialidad de los algoritmos en el análisis de los metadatos. Primeramente, un estudio de Kosinski-Stillwell-Graepel (2012) publicado en *Proceedings of the National Academy of Sciences of the United States of America*, mostró que los *likes* que otorgamos en las redes sociales son capaces de desvelar datos sensibles acerca de nuestros gustos y preferencias en lo relativo a sexualidad, política, religión y estado civil. Este articulo puso en evidencia la capacidad de los algoritmos inteligentes para conocer de manera indirecta datos sensibles de los individuos. A través del análisis pormenorizado de la interacción de los usuarios con los contenidos de *Facebook* se puede discriminar con un importante grado de precisión las preferencias personales.

Otro artículo firmado por Kramer-Guillory-Hancock (2014) mostró de qué manera las emociones, ya sean positivas o negativas, son contagiadas entre los usuarios a través de la simple visualización de los mensajes, influyendo en su comportamiento interactivo. Este estudio ha sido pionero en la demostración del contagio emotivo a través del lenguaje escrito, sin la intervención de elementos verbales. Las técnicas desarrolladas podrán ser utilizadas para la manipulación de la opinión pública, o bien, para ofrecernos productos con publicidad personalizada cuyo objetivo es estimular emocionalmente a los consumidores.

Finalmente, un estudio de Youyou-Kosinski-Stillwell (2015) ha mostrado que un algoritmo informático es capaz de calcular mejor la personalidad de un usuario que un colega de trabajo usando 10 likes, mientras que con 150 es capaz de dar una descripción más detallada que los hermanos o los padres. La capacidad de los algoritmos mencionados para clasificar a los usuarios, predecir sus comportamientos o para influir sobre su percepción los convierte en potenciales *riesgos tecnológicos*. Lo deseable es que estas herramientas no se pongan en manos de regímenes antidemocráticos o en empresas con prácticas que violenten los derechos fundamentales de los usuarios.

En un futuro inmediato podemos esperar que el desarrollo de nuevos instrumentos tecnológicos permitirán una amplia gama de usos con la información obtenida mediante el análisis de datos y metadatos. En algunos casos específicos esa información servirá no solamente para otorgar datos personales, sino también para definirnos caracterialmente y hasta para predecir algunos comportamientos o tendencias de opinión. Ante esto surgen diversos problemas éticos-jurídicos. Probablemente uno de los más importantes consiste en definir apropiadamente la posesión y usos legítimos de esos datos, para evitar que puedan ser usados en acciones que lesionen la libertad y los derechos fundamentales de las personas.

3. Regulación de datos en México y el caso Facebook

Estudiar la regulación de los datos personales en México requiere un enfoque a varios niveles. Primeramente se pueden considerar los instrumentos jurídicos internacionales que han inspirado a las legislaciones domésticas, para determinar algunos estándares de referencia. Después, se puede explorar el nivel constitucional y la forma en la que se expresa en la legislación secundaria. En tercer lugar, es necesario analizar la capacidad y las condiciones en la que diversos organismos públicos pueden acceder a los datos personales d de los usuarios de internet. En cuarto lugar, es importante conocer el marco jurídico que regula la recopilación, análisis y uso de los datos personales por parte de entidades privadas.

En el presente apartado se llevará a cabo un breve repaso respecto a los diferentesniveles de análisis. El objetivo de esta síntesis consiste en mostrar que en los hechos empresas privadas como las redes sociales recaban todo tipo de información de los usuarios, especialmente información sensible, pero también en señalar en qué circunstancias las autoridades mexicanas han tenido acceso a lo metadatos de los ciudadanos.

La regulación de la recolección y uso de datos personales se inspira principalmente en la *Declaración Universal* de la Asamblea General de la ONU de 1948. En su art. 12 se 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. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". En este primer referente se define que la injerencias públicas legítimas no deben implicar de ningún modo la lesión de los derechos a la privacidad y la intimidad.

El principio de *presunción de inocencia* puede considerarse como uno de los pilares esenciales de la democracia moderna, ya que garantiza las libertades civiles fundamentales.[138] Su consolidación impactó, de hecho, en la creación de normas para regular otros derechos como la comunicación y la propiedad. En relación a la propiedad, considerado desde las revoluciones burguesas como el derecho civil por excelencia, las sociedades democráticas han garantizado progresivamente el uso legítimo del patrimonio personal dando amplia libertad a la realización de cualquier acción que no implicase actos ilícitos. El derecho a la privacidad o a la intimidad puede considerarse el producto de la unión del principio de presunción y del derecho a la propiedad. El domicilio particular se convirtió desde entonces en una especie de recinto sagrado que debía salvaguardarse de las arbitrariedades del Estado o de las cambiantes mareas políticas. Nadie podía invadir ese recinto sagrado, sino solamente mediante orden judicial previa que justificase debidamente la intromisión en la vida privada.

Las leyes que regulaban la libertad de comunicación en la época en la que la mayor parte de la población debía comunicarse con tecnologías rudimentarias como las cartas en papel o las llamadas telefónicas no procesadas mediante sistemas informáticos, establecían también que el ámbito de la privacidad abarcaba ese tipo de comunicaciones. Las comunicaciones personales, eran una extensión del domicilio particular, de la vida íntima de los individuos, por lo que intervenirlas podía considerarse como un medio ilegítimo e ilegal de vigilancia. Naturalmente, esto funcionaba así en las sociedades que habían alcanzado un progreso importante en el Estado de Derecho, mientras que en los regímenes totalitarios existía una fuerte inversión para espiar a los disidentes políticos.

Inspirándose en la *Declaración Universal*, la reforma del 2008 al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, establece que "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 dicho artículo se dice también que todas las personas tienen derecho a la protección de sus datos personales, así como al acceso, rectificación y cancelación de los mismos. El documento constitucional es muy específico en el sentido de

[138] Ver Gigliola, Maria (2016) "Quale scienza penale? Prima e dopo Beccaria, en Flora Giovanni (comp.) *Dei delitti e delle pene a 250 anni dalla publicazione. La lezione di Cesare Beccaria,* Giuffrè Editore, pp, 146 y ss

que solamente la autoridad judicial federal podrá autorizar la intervención de cualquier comunicación privada, definiendo que las causas legales de la solicitud deberán ser explícitas en la orden judicial, así como el tipo de intervención permitido, las personas implicadas y la duración. Asimismo, la posibilidad de usar este recurso se excluye en casos electorales, fiscales, mercantiles, civiles, laborales, administrativos y las comunicaciones del detenido con su defensor.

Por su parte, el *Pleno del Instituto Federal de Acceso a la Información Pública*, (con fundamento en los artículos 15, 16 y 37, fracción III de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 28 y 64 de su Reglamento) emitió los *Lineamientos Generales para la Clasificación y Desclasificación de la Información de las Dependencias y Entidades de la Administración Pública Federal*. En el art. 32 se establece que:

> "será confidencial la información que contenga datos personales de una persona física identificada o identificable relativos a: origen étnico o racial, características físicas, morales y emocionales, vida afectiva y vida familiar, domicilio y número telefónico particular, patrimonio, ideología, opinión política, creencia o convicción religiosa o filosófica, estado de salud físico y mental, preferencia sexual, y otras análogas que afecten su intimidad, como la información genética".

Por su parte, la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, desarrolla parcialmente el artículo 16 constitucional, pues específica las reglas del almacenamiento y uso de datos solamente para personas físicas y morales de carácter privado. En dicha ley se define como *dato personal*: "cualquier información concerniente a una persona física identificada o identificable". Por su parte, los *datos personales sensibles* son considerados como:

> "aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual".

A su vez, la ley regula la necesidad de los avisos de privacidad ordenando la transparencia respecto a la identidad y domicilio del recaudador de datos, los objetivos del tratamiento de los datos, las formas de limitación para el uso o divulgación, los medios para acceder, rectificar, cancelar u oponerse, así como los procedimientos para comunicar los cambios en los avisos de privacidad. En realidad la ley mexicana contempla solamente estos mecanismos de creación de normas unilaterales o pactos de adhesión, en los que

el usuario tiene nulas posibilidades de participar activamente en la formulación de las reglas. Este es el caso específico de *Facebook* y *Whatsapp*, que en sus contratos de adhesión establecen una cláusula que indica que el usuario concede trasladar a un tribunal en California cualquier querella legal. En la última *Declaración de Derechos y Responsabilidades*, actualizada el 30 de enero de 2015 se puede leer:

> "Resolverás cualquier demanda, causa de acción o conflicto (colectivamente, "demanda") que tengas con nosotros surgida de o relacionada con la presente Declaración o con Facebook únicamente en el tribunal del Distrito Norte de California o en un tribunal estatal del Condado de San Mateo, y aceptas que sean dichos tribunales los competentes a la hora de resolver los litigios de dichos conflictos. Las leyes del estado de California rigen esta Declaración, así como cualquier demanda que pudiera surgir entre tú y nosotros, independientemente de las disposiciones sobre conflictos de leyes".[139]

En 2015, Shore-Steinman firmaron un artículo acerca de la evolución de las políticas de privacidad en *Facebook* concluyendo que ha existido un importante empeoramiento desde el 2005 hasta el 2015, al ser menos transparente y más difícil de entender para los usuarios, incluyendo la opción sobre el uso de la información personal frente a terceros (empresas privadas o agencias gubernamentales). Las políticas de privacidad están redactadas de tal modo que la mayor parte de las responsabilidades recaen sobre el propio usuario, ya que las empresas renuncian a garantizar la privacidad de los mismos ya sea por peticiones de *buena fe* de agencias gubernamentales, por el uso de los datos de otras aplicaciones o por errores técnicos. La información recibida pertenece a cuatro grandes sectores que son: 1) Los datos personales (algunos sensibles) publicados por el usuario, 2) Los recopilados a través del navegador (tipo de navegador, IP y cookies), 3) Datos de geolocalización y 4) Datos publicados por el usuario en otras plataformas y blogs.[140]

En el siguiente cuadro se presenta una breve sinopsis de las políticas de privacidad vigentes actualmente en la red social con mayor número de usuarios (*Facebook*):

[139] El texto completo se puede consultar en: https://www.facebook.com/legal/terms

[140] Shore J, Steinman (2015) "Did You Really Agree to That? The Evolution of Facebook's Privacy Policy". En *Technology Science*. 2015081102. August 11, 2015. En: https://techscience.org/a/2015081102

Grupos	Tipo de información recopilada	Usos	Cómo se comparte
Datos y metados de interacción propios	Actividad e información proporcionada voluntariamente (incluye contenido de mensajes “privados”)	Personalización de contenido y sugerencias. Proporcionar, mejorar y desarrollar los servicios	Personas con las que el usuario se comunica y comparte contenido
Datos y metadatos de otros	La actividad de otros usuarios y la información que proporcionan (incluye contenido de mensajes “privados”)	Marketing aplicado: envio de mensajes de publicidad a los usuarios	Personas que ven contenido que otros usuarios comparten
Datos sociométricos	Informaciòn sobre las redes personales y las conexiones	Estudios de marketing: mostrar y medir anuncios y servicios	Aplicaciones, sitios web e integraciones de terceros que usan los servicios
Datos bancarios	Número de tarjeta y otra información sobre la tarjeta, datos sobre la cuenta y autenticación, datos de facturación, envío y contacto.	Fomentar la seguridad y protecciòn	Se comparte informacòn dentro de las empresas de Facebook
Geolocalización y datos de conexión	Datos dispositivos de conexión (sistema operativo, versiòn de hardware, configuración, tipos de programas, cargas de baterías, intensidad señal, identificación del dispositivo), geolocalización, información específica conexión (proveedor, ip, número de teléfono, idioma)		Nuevos propietarios: Si cambian la propiedad o el control de la totalidad o de parte de nuestros Servicios o de sus activos, podemos transferir tu información al nuevo propietario
Sitios web y empresas que usan servicios Facebook	Información de interacción de “me gusta”, inicio de sesión o servicios de medición y		Servicios de publicidad, medición y análisis (solo información

	publicidad.		que no permita la identificación personal)
Socios externos	Información que proporcionan socios.		
Empresas Facebook	Datos que proporcionan otras empresas pertenecientes u operadas por Facebook.		

Para evitar que toda esta información pueda servir como un instrumento para que las autoridades lesionen los derechos fundamentales, la resolución emitida por la *Asamblea General de la ONU* con nombre *El derecho a la privacidad en la era digital* del 18 de diciembre de 2013, recomienda a los Estados la creación de "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". En este sentido, el sistema jurídico mexicano se encuentra por debajo de los estándares internacionales para la protección de la privacidad y la intimidad, pues no contempla la existencia de mecanismos civiles e independientes de supervisión.

Además de lo mencionado, la *Declaración conjunta del Relator Especial sobre el derecho a la libertad de opinión y expresión de la ONU con la Relatora de la Comisión Interamericana sobre Derechos Humanos*, señala que:

> "Toda persona tiene derecho a acceder a información bajo el control del Estado. Este derecho incluye la información que se relaciona con la seguridad nacional, salvo las precisas excepciones que establezcan la ley siempre que estas resulten necesarias en una sociedad democrática…los Estados deben difundir, por lo menos, información relativa al marco regulatorio de los programas de vigilancia, los órganos encargados para implementar y supervisar dichos programas: los procedimientos de autorización, de selección de objetivos y de manejo de datos, así como información sobre el uso de estas técnicas, incluidos datos agregados sobre su alcance. En todo caso, los Estados deben establecer mecanismos de control independientes capaces de asegurar transparencia y rendición de cuentas sobre estos programas".

Por su parte, la *Ley General de Transparencia y Acceso a la Información Pública* contempla en el artículo 70 que las empresas de telecomunicaciones deben proporcionar información para efectos estadísticos acerca de las intervenciones de comunicaciones privadas, el acceso al registro de telecomunicaciones y la geolocalización en tiempo real. Actualmente todas las entidades federativas han adecuado su normatividad para ser compatibles con la ley federal, pero los resultados prácticos no son los que se esperaban. Esta ley establece además que la información estadística sobre medidas de vigilancia debe ser publicada proactivamente por la autoridad competente así como en la *Plataforma Nacional de Transparencia*, siendo actualizada al menos cada tres meses.

Por su parte, los *Lineamientos de Colaboración en Materia de Seguridad y Justicia* del *Instituto Federal de Telecomunicaciones* establece las obligaciones de las empresas con concesión y de las autoridades correspondientes respecto a la transparencia. Las empresas y las autoridades implicadas en la vigilancia se encuentran obligadas a entregar dos informes anuales al IFT, los cuales deberían ser de acceso público. No obstante, el plazo de cumplimiento se prorrogó de noviembre de 2016 a mayo del 2017, por lo que aún no se cuentan con datos oficiales sobre estas prácticas.

En el informe de una organización civil por los derechos civiles (R3D) queda claro que el IFT "no ha cumplido con la obligación asumida por sí mismo de solicitar a las autoridades un informe semestral".[141] La misma organización denuncia una cultura de opacidad generalizada por parte de las autoridades mexicanas, ya que en algunos casos agencias como el *CISEN* se negaron a dar información de sus actividades.

Los casos documentados demuestran que entre 2013 y 2015, se realizaron 3182 solicitudes de autorización judicial para la intervención de comunicaciones privadas, de las cuales solamente el 5.28% fueron rechazadas. Resulta importante resaltar que una solicitud puede incluir la vigilancia de múltiples dispositivos y personas. En el informe también se muestran inconsistencias importantes, pues los datos de las procuradurías locales se contradicen con los datos aportados por el *Consejo de la Judicatura Federal*. R3D denunció, finalmente, que además de los problemas relacionados con la transparencia, el uso de medidas de vigilancia no han desembocado en ejercicios de acción penal, por lo que parece que la mayor parte de las personas vigiladas jamás son llevadas a juicio (solamente el 8.73% culminan en procedimiento).

[141] R3d Red en Defensa de los Derechos Digitales (2016) *Reporte*: *El Estado de la Vigilancia. Fuera de Control*, México , p. 36.

Ante esta situación, resulta preciso preguntarnos acerca de los tipos de vigilancia regulados por la ley mexicana. Pueden distinguirse, al menos, los siguientes:

1. Geolocalización en tiempo real a través de equipos de comunicación móvil. *Ley Federal de Telecomunicaciones y Radiodifusión* (art. 190, fracción I); el *Código Nacional de Procedimientos Penales* (art. 303) y los *Lineamientos de Colaboración en Materia de Seguridad y Justicia* del IFT (Cap. III). El Amparo 264/2015 frente a la SCJN dijo que esta medida puede utilizarse exclusivamente en los casos en los que "se presuma que existe un peligro para la vida o integridad de una persona".

2. Intervención de comunicaciones privadas: *Constitución Política* (art 16) y *Código Nacional de Procedimientos Penales* (art. 291): "La intervención de comunicaciones privadas, abarca todo sistema de comunicación o programas que sean resultado de la evolución tecnológica que permitan el intercambio de datos, informaciones, audio, vídeo, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real". *Ley General para Prevenir y Sancionar los Delitos en Materia de Secuestro* (art. 24), *Ley Federal contra la Delincuencia Organizada* (art. 48-55), *Ley de Seguridad Nacional* (Art 33-49), *Código Militar de Procedimientos Penales* (art. 287)

3. Conservación obligatoria de metadatos de comunicaciones: *LFTR* (art. 190, fracción II): Conservación por 24 meses de datos de tráfico de telecomunicaciones.

Por su parte, las agencias que están facultadas para acceder a los datos y para vigilar, previo mandato judicial, son:

1. La Procuraduria General de la República y los procuradores de las entidades federativas: *CNPP* del 292 al 302. Cuando se considere indispensable para la investigación de algún delito,.

2. La Policía Federal: *Ley de la Policía Federal* (art. 48 al 55): Cuando se constate la existencia de indicios suficientes que acrediten que se está organizando la comisión de ciertos delitos. Algunos ejemplos son espionaje, sabotaje, terrorrismo, rebelión, traición a la patria, genocidio, actos de interferencia extranjera en asuntos nacionales, actos contra los poderes o contra las operaciones militares, navales o de la aviación, actos contra el personal diplomático o de contrainteligencia, así como la destrucción o inhabilitación de infraestructura estratégica.

3. El Centro de Investigación y Seguridad Nacional: *Ley de Seguridad Nacional* (art. 33) establece que se pueden intervenir las comunicaciones privadas, cuando existan casos de amenaza a la seguridad nacional, definidos en el art.

Los datos proporcionados por las autoridades federales para el acceso a los datos conservados muestra que de todas las solicitudes solamente 1.09% contaban con autorización judicial federal, por lo que la mayor parte de las acciones de vigilancia se realizaron en condiciones discutibles ética y jurídicamente. A esto se puede agregar que de todas las solicitudes realizadas, las empresas solamente rechazaron el 8.29%. Esto es especialmente preocupante en entidades federativas como Chihuahua y Veracruz que concentran una gran parte del acceso a la geolocalización, siendo territorios en los que se han dado sistemáticas violaciones a los derechos fundamentales como asesinatos y desapariciones de periodistas.

La regulación federal para las telecomunicaciones establece, por ejemplo, que todos los metadatos de las telecomunicaciones, es decir, información acerca de las comunicaciones personales de los ciudadanos deben ser almacenadas por los prestadores de servicios a lo largo de 48 meses (*Ley Federal de Telecomunicacione*s, art. 190, fracc. II). También ha dispuesto las reglas para la intervención directa de telecomunicaciones privadas y la geolocalización en tiempo real, abriendo las puertas a un tipo de vigilancia indiscriminada (art. 190 fracciones I y II).

A esto se puede agregar que la regulación se empeña en fortalecer los mecanismos de vigilancia disponibles para las empresas prestadoras de servicios, así como para agencias estatales autorizadas a tener acceso a los datos (PGR, Procuradurías estatales, PFP y CISEN), pero no establece claramente cuáles son los derechos de los ciudadanos, ni mucho menos los mecanismos de protección de las garantías que materializarían esos derechos. Se trata de un déficit importante en el desarrollo de la protección y tutela de los derechos digitales en beneficio de la vigilancia. Finalmente, algunos reportes de organizaciones no gubernamentales como R3D evidencian que las normas de transparencia han presentado muchas deficiencias derivadas de los obstáculos para acceder a las cifras en poder de las empresas y las agencias gubernamentales. En algunos casos específicos, los datos que se han podido obtener reflejan importantes incongruencias.[142]

4. A manera de conclusión

Desde el punto de vista jurídico, cuando se recolectan y almacenan metadatos indiscriminadamente como en México se lesionan algunas de las garantías fundamentales establecidas por los estándares internacionales. En

[142] *Ibid*, pp. 29-35.

primer lugar, se encuentra el problema de que no todas las acciones de vigilancia han sido llevadas a cabo respetando el requisito del mandato judicial previo. En segundo lugar, un problema preocupante es el referente a la imposibilidad de las personas de saber que están siendo sujetas a una vigilancia al no existir notificación diferida de los afectados. Finalmente, un asunto pendiente es la cuestión de la transparencia de los organismos privados y públicos que amparándose en la justificación de la *seguridad nacional* se niegan a hacer pública la información referente a la vigilancia, así como la inexistencia de un organismo de supervisión independiente que vele por la protección del derecho a la privacidad de las personas.

Entre las obligaciones fundamentales de estos organismos se encuentran la publicación de informes periódicos de las empresas prestadoras de servicios en las que se establezca con toda claridad cuántas peticiones de vigilancia y acceso a los metadatos se realizan por parte de las autoridades competentes y cuántas se conceden. Por otra parte, las autoridades deberían realizar también la publicación de informes periódicos en los que se esclarezca toda esta información para que las organizaciones de la sociedad civil y los propios ciudadanos puedan estar plenamente conscientes de la penetración de la vigilancia. En este sentido, los *Principios Globales sobre Seguridad Nacional y Derecho a la Información* firmados en Tshwane establecen que debe existir claridad en lo referente a: 1) las leyes que rigen todos los tipos de vigilancia; 2) los objetivos permisibles de la vigilancia; 3) el umbral de sospecha requerido ; 4) limites temporales; 5) procedimientos para la autorización; 6) especificación de los tipos de datos a recabarse; y 7) los criterios que se aplican al uso, retención, eliminación y transferencia de los datos.

La vigilancia debería supeditarse al cumplimiento de los principios de necesidad y proporcionalidad. Esto tiene sentido si pensamos que solamente en un marco legal y procedimental que ponderé las peticiones de vigilancia bajo esos criterios puede ser legítima la vigilancia. En primer lugar, el principio de necesidad establece que la vigilancia se debe aplicar únicamente cuando no existan alternativas viables y menos lesivas para conseguir un fin legítimo, como puede ser proteger la vida y la seguridad de las personas. En segundo lugar, el principio de proporcionalidad indica que la vigilancia es legítima solamente cuando no resulte exagerada o desmedida frente a las posibles ventajas que se puedan obtener de su aplicación.

Los procedimientos que favorecen la privacidad y la intimidad de las personas son la notificación del implicado y los mecanismos de supervisión ciudadana de las agencias encargadas de la vigilancia. Los procedimientos que favorecen el argumento de la *seguridad nacional* son el uso de todas las medidas de vigilancia que no lesionen los derechos fundamentales de las personas y que no hagan uso de tecnologías ilegales o éticamente problemáticas como los programas espías.

FUENTES

Assange, Julian (2013) *Internet è il nemico*, Feltrinelli, Milano.

Bernstein, Jeremy (1990) *Uomini e macchine intelligenti*, Adelphi, Milano

Brand Finance (2017) *Global 500. The annual report on the wolrd's most valuable brands*, en: www.brandfinance.com

Bumiller, Elisabeth (2010) "Video Shows U.S. Killing of Reuters Employees", *The New York Times*, 05/04/2010. En http://www.nytimes.com/2010/04/06/world/middleeast/06baghdad.html

Farouk, Yasmine (2012) "La revolución de Egipto: muy pronto para concluir, a tiempo para excluir", en *Foro Internacional*, El Colegio de México, núm. 2

Ferraris, Maurizio (2008) *¿Dónde estás? Ontología del teléfono móvil*, Marbot, Barcelona.

Gigliola, Maria (2016) "Quale scienza penale? Prima e dopo Beccaria, en Flora Giovanni (comp.) *Dei delitti e delle pene a 250 anni dalla publicazione. La lezione di Cesare Beccaria,* Giuffrè Editore

Kang, Cecilia (2017) "Congress Moves to Strike Internet Privacy Rules From Obama Era", *The New York Times,* 23/03/2017. En: https://www.nytimes.com/2017/03/23/technology/congress-moves-to-strike-internet-privacy-rules-from-obama-era.html

Keen, Andrew (2013) *Vertigine digitale. Fragilità e disorientamento da social media*, Egea, Milano.

Kosinsky, Stilwell y Graepel (2012) "Private traits and attributes are predictable from digital records of human behavior", en *Proceedings of the National Academy of Sciences of the United States of America*, vol. 110, no. 15.

Kramer, Guillory y Hancock (2014) "Experimental evidence of massive-scale emotional contagion through social networks", en *Proceedings of the National Academy of Sciences of the United States of America*, vol. 111, no. 24.

Ley Federal de Telecomunicaciones y Radiodifusión. Consultada en: http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014

Lorcan Dempsey and Stuart L.Weibel (1996) *The Warwick Metadata Workshop: A Framework for the Deployment of Resource Description. D-Lib Magazine*, July/August 1996. http://www.dlib.org/dlib/july96/07weibel.html

Lou Burnard et al (1996) *A Syntax for Dublin Core Metadata: Recommendations from the Second Metadata Workshop*. April 1996. http://www.uic.edu/~cmsmcq/tech/metadata.syntax.html

Moore, Gordon (1965) *Cramming more components onto integrated circuits*, in: *Electronics*, vol. 38, n. 8, apr. 19-1965

Pratt, Vernon (1990) *Macchine pensanti. L'evoluzione dell'intelligenza artificiale*, Il Mulino .

R3d Red en Defensa de los Derechos Digitales (2016a) *Reporte*: *El Estado de la Vigilancia. Fuera de Control*, México .

R3d Red en Defensa de los Derechos Digitales (2016b) *¿Quién defiende tus datos? Reporte de evaluación de empresas de telecomunicaciones ante las medidas de vigilancia*, México.

Shore J, Steinman (2015) "Did You Really Agree to That? The Evolution of Facebook's Privacy Policy". En *Technology Science*. 2015081102. August 11, 2015. En: https://techscience.org/a/2015081102

Stöcker, C, y Lischka, K (2013) "New Leaks Show Near Total NSA Surveillance", *Spiegel online*, 01/08/2013. En: http://www.spiegel.de/international/world/new-nsa-leaks-describe-total-surveillance-system-xkeyscore-a-914244.html

Youyou, Kosinski y Stillwell (2014) "Computer-based personality judgments are more accurate than those made by humans" en *Proceedings of the National Academy of Sciences of the United States of America,* vol. 112, n. 4.