Derechos humanos en internet en México: violación y desposesión

Mariana Celorio*

La violación y desposesión de derechos humanos (DH) en internet en México son el eje de este trabajo. Aquí la autora analiza cuándo el espionaje electrónico y la videovigilancia violan DH y cuándo los desposeen; indaga en qué sentido las *cookies* y los *web bugs* son dispositivos ilegales de recolección de información y en qué sentido violan la propiedad privada de los usuarios de internet y cómo transformaron internet. Establece que la violación y la desposesión de DH obedecen a una racionalidad biopolítica que produce estados de excepción en espacios reales y en territorios digitales. Inserta el análisis en la discusión sobre la obligación de que actores no estatales respeten los DH y se pregunta si es posible hablar del capital como actor que viola DH en internet.

Introducción

En este trabajo analizo la relación entre internet[1] y derechos humanos (DH) en México durante las últimas dos décadas, periodo que lleva el uso de esta tecnología en el país. Para ello, parto de dos premisas fundamentales: en la primera afirmo que existen violaciones de DH en y a través de internet y en la segunda sostengo que existe desposesión de DH en el capitalismo contemporáneo y la confronto aquí en términos empíricos, en este caso, en internet.

Respecto a la primera, la categoría de violación de DH goza plenamente de consenso; sin embargo, la categoría conceptual que propongo en una investigación previa colisiona con tradición en la aproximación a los DH y con la ortodoxia y rigidez del derecho positivo y de la teoría jurídica. Para los abogados no puede existir desposesión de derechos, porque, según ellos, los derechos por ningún motivo se pierden, sólo se violan y frente a esto existe la figura de "reparación del daño". Sin embargo, desde la sociología política y mediante un sensible ejercicio de abstracción crítica, encuentro una nueva realidad frente a la cual la categoría "violación de DH" no es suficiente para explicar lo que sucede en México y en muchas otras partes del mundo, y que esta nueva realidad implica una nueva conceptualización teórica, la desposesión de DH; esto es, en el marco del sistema nacional e internacional de DH, el sistema político mexicano construye nuevos ordenamientos legales para operar tanto al capitalismo contemporáneo como al Estado de seguridad, incompatibles con los DH de individuos, pueblos y comunidades.

A partir de estas dos distinciones, violación y desposesión, analizo qué ha pasado con los DH en internet. Para ello estructuré este trabajo en tres secciones; en la primera reviso la categoría violación de DH y explico la categoría desposesión de DH, donde enfatizo que es una propuesta conceptual que emana de una sociología crítica de las relaciones de poder; en la segunda sección analizo a los usuarios de internet en México para dimensionar a

* Este artículo es parte de los resultados de la investigación sobre la desposesión del DH en el capitalismo contemporáneo que realizó en la estancia de posdoctorado en la Universidad Iberoamericana, como becaria del Conacyt. Correo electrónico: <celoriom@hotmail.com>.

[1] Internet, como lo conocemos hoy, en su protocolo *www*, fue creado en 1989 por Tom Lee y Vinton Cerf; 10 años después, en 1999, internet aún era incipiente en México. Universidades públicas y privadas encabezadas por la UNAM se esforzaban por difundirlo.

la comunidad de usuarias y usuarios que interactúan en y a través de internet; en la tercera sección presento de manera simultánea la violación y la desposesión de DH en internet y los contrasto con ejemplos concretos derivados de leyes específicas y de notas periodísticas.

Por último, es necesario comentar cuatro precisiones de carácter metodológico:

a) Sustento el análisis sobre la relación entre DH e internet en la "resolución aprobada en 2012 por el Consejo de DH de la ONU que sostiene que todos los derechos que tienen las personas físicas deben ser protegidos también en el ámbito digital" (Hoffman, 2012).
b) Concibo la desposesión de DH como un dispositivo biopolítico (Foucault) de control y administración de poblaciones y territorios y, en este sentido, veo a internet como un territorio público de interacción social y frente a la violación y desposesión donde se producen estados digitales de excepción intangibles para las *víctimas*.
c) Frente a discursos dominantes de seguridad pública y terrorismos, hay riesgo de normalizarla y legitimarla.
d) No abordo la Web Profunda por no tener la posibilidad para navegar con seguridad en este nivel de internet.

Conceptualización de violación y desposesión de DH

Hablar de violación de DH no es sencillo en virtud de que es una situación que no sólo tiene que ver con el actor que vulnera derechos, con el tipo de derechos que se vulneran, con el objetivo que se persigue y con las consecuencias que producen dichas violaciones.

La noción violación de DH es lugar común; sin embargo, cuando se problematiza en torno a quién es el actor que viola DH, se complica su aprehensión. Las preguntas que surgen aquí son: ¿el capital[2], vía sus gerentes y mercenarios, puede ser considerado como un actor que viola DH? ¿El crimen organizado viola DH? ¿El empresario o patrón viola DH? ¿La sociedad civil y los movimientos sociales pueden ser vistos como entidades que violan DH? Para aproximarnos a una respuesta, el trabajo de Clapham da pistas que permiten argumentar que si actores no estatales violan DH debieran responder por las violaciones que comenten y debieran ser considerados como actores que violan DH, si bien inserta su trabajo en los beligerantes, los movimientos de liberación nacional y los grupos insurgentes, argumentando que estos grupos armados en tiempos de conflicto deben responder por las violaciones de DH que comenten. "Cada vez son más las expectativas en cuanto a que todos los actores no estatales respeten los principios del derecho internacional de los derechos humanos" (Clapham, 2006).

Si bien su trabajo está enfocado a conflictos armados internos, es necesario trabajar hacia la aceptación de que si hay violación de derechos, todos los actores involucrados, sean estatales o no estatales, son entidades que violan derechos humanos, y no sólo depositarle la obligación de respetar DH a actores estatales.

Ahora bien, se entiende por violación de DH al acto que realiza un agente estatal que transgrede o va en contra de cualquier DH consignado en la Declaración Universal de Derechos Humanos, en el Pacto de Derechos Económicos, Sociales y Culturales (DESC) y en todos los demás protocolos firmados y ratificados.

La violación de DH puede ser por acción, por omisión y por exclusión. La violación por acción[3] es cuando un agente estatal, amparado en la fuerza del poder del Estado, ataca directamente a una persona, comunidad o población. Cuando, recordando a Agamben, el sujeto puede ser violentado es inservible para los intereses dominantes, es una amenaza a la reproducción de las condiciones de acumulación de la riqueza y puede ser prescindible; el agente estatal administra y gestiona poblaciones y decide quién vive y quién muere (Agamben, 2007).

La violación por omisión sucede cuando "los poderes públicos o sus agentes –o, en general, las personas que tienen el deber de respetar y proteger los derechos– se muestran indiferentes frente a situaciones que reclaman su intervención. Es el caso, por ejemplo, de aquellas políticas económicas que no garantizan el derecho a un nivel de vida digno, el derecho al trabajo o el derecho a la educación" (Cubaencuentro, s/a), y también permitir la violación del derecho a la privacidad en internet y no hacer nada al respecto.

[2] Para efectos de este trabajo, la violación y desposesión de DH cometidas por el capital apuntan a contribuir al debate acerca de si deben ser considerados como un actor que viola y desposee DH.

[3] "Una violación de los derechos económicos, sociales y culturales tiene lugar cuando un Estado incumple sus obligaciones de garantizar que tales derechos se disfruten sin discriminación o su obligación de respetarlos, protegerlos y realizarlos. Frecuentemente una violación de tales derechos guarda relación con la violación de otros derechos" (OHCHR, s/a).

Considero necesario hacer un esfuerzo de análisis crítico respecto al enfoque tradicional de la omisión; es decir, me parece que también debiera ser considerada violación por omisión cuando los agentes estatales permiten que un actor económico, social, religioso o criminal viole por acción DH. Un ejemplo de ello para entornos digitales es el espionaje electrónico del sector patronal-empresarial a sus empleados y sindicatos.

La violación por exclusión "tiene lugar cuando determinadas capas de la población son explícitamente marginadas del goce de los derechos. Esta situación puede ser sufrida a causa del sexo, de la religión profesada, de la raza, de la nacionalidad, de la edad, de la clase social a la que se pertenece, al nivel económico que se tiene, etc." (Cubaencuentro, 2016).

Cuando hablamos de violación por acción, omisión y exclusión en el mundo tangible y material, resulta relativamente más sencillo identificarlo y nombrarlo. Es decir, por acción, la tortura; por omisión, las consecuencias sociales de la desigualdad; por exclusión, el maltrato y discriminación a personas con capacidades diferentes. Los anteriores algunos ejemplos; sin embargo, cuando hablamos de violación de DH en internet, se vuelve mucho más compleja su identificación; resulta muy difícil darse cuenta, nombrarlo, denunciarlo, defenderlo y reivindicarlo, sobre todo cuando se trata de Estados digitales de excepción, entendiendo por éstos sitios y aplicaciones en internet donde se violan y se desposeen DH y se incumplen ordenamientos legales, dejando en estado de indefensión a los perfiles demográficos afectados y que, por la dificultad de la materia informática y porque el espionaje y la vigilancia electrónica no dejan rastro visible para quienes no son expertos en la materia, estas poblaciones no se percatan y, si lo hacen, difícilmente pueden asociarlo a un DH específico y reivindicarlo.

Un ejemplo de ello es el sistema operativo Windows 10, que tiene funciones asociadas para espiar a sus usuarios y se instala en los equipos de manera automática. Los usuarios no necesariamente saben que Windows 10 incluye un programa espía y, mientras lo usan, entregan, sin saberlo, su información, que por definición es confidencial. "El nuevo sistema operativo de Microsoft constantemente monitorea la actividad del usuario y recopila información de uso con el fin de hacerla llegar a la compañía. A pesar de que en internet circulan diversos tutoriales para desactivar las funciones de rastreo de actividad, Joe Belfior, vicepresidente ejecutivo de Microsoft, dijo que no es posible evitar que Windows 10 envíe información de uso a la empresa" (Ortega, 2015).

Si el capital fuera un actor considerado como ente que viola DH, se podría hablar de que Microsoft viola por acción la intimidad y la privacidad de sus usuarios, mientras que el gobierno de México viola por omisión el derecho a la intimidad y a la privacidad de más de 20 millones de personas que usan Windows 10, cifra estimada luego de la declaración, en 2015, de Ruperto Torre, gerente de Producto de Windows: "En México hay 23 millones de usuarios corriendo Windows 7 y Windows 8 en sus computadoras. Nuestro objetivo es llegar a estos mexicanos que lo puedan descargar sin costo en este primer año" (Chávez, 2015).

Si hablar de violación de DH en internet es complejo, hablar de desposesión de DH en internet lo es aún más, pues requiere un ejercicio de abstracción que desarrollo en el siguiente apartado, pero antes retomo mi conceptualización sobre la categoría analítica de desposesión de DH que cito a continuación de un texto anterior[4]:

> Por tratarse de procesos causales o paralelos, baso mi conceptualización de Desposesión de Derechos Humanos en la categoría de acumulación por desposesión de Harvey, quien a su vez ofrece una explicación ampliada de la acumulación originaria de Marx. ["La acumulación por desposesión incluye la mercantilización y privatización de la tierra y la expulsión forzosa de las poblaciones campesinas, la conversión de diversas formas de derechos –de propiedad, común, colectiva, estatal, etc.– en derechos de propiedad exclusivos […] la transformación de la fuerza de trabajo en mercancía y la supresión de formas de producción y consumo alternativas; los procesos coloniales, neocoloniales e imperiales de apropiación de activos, incluyendo los recursos naturales; El estado, con su monopolio de la violencia y sus definiciones de legalidad, juega un rol crucial al respaldar y promover estos procesos"] (Harvey, 2004).

Quitarles a los otros lo que tienen y usarlo de acuerdo con lógicas de rentabilidad económica es en sí mismo un proceso violento e incompatible con los derechos humanos.

[4] Celorio Suárez Coronas, Mariana (2016, Mimeo), "Desposesión de derechos humanos en el capitalismo contemporáneo", en Estévez, Ariadna, y Vázquez, Daniel, *El capitalismo neoliberal y sus descontentos: 10 razones para (des)confiar de las luchas por los derechos humanos*, UNAM/Flacso.

En democracias capitalistas, violar derechos es un acto que desprestigia a sus actores y los obliga a dar cuenta de ello; en contraste, suprimir derechos allana el camino para las dinámicas estratégicas de acumulación capitalista, que no es factible en esquemas éticos y legales de respeto y protección de los DH. Por ello, acoplo la reflexión de Harvey sobre la acumulación por desposesión a la desposesión de derechos humanos. La concibo como una estrategia del proyecto neoliberal para la privatización de territorios y de recursos [y en el caso de internet, de la apropiación de territorios digitales].

La desposesión de derechos humanos es: a) una acción consciente que élites políticas y económicas realizan a través de una racionalidad biopolítica mediante la cual sustraen DH; b) persigue la reconfiguración territorial de acuerdo con las actividades estratégicas de acumulación, explotación y producción; y c) se basa en la producción de ordenamientos jurídicos como instrumentos para operar ajustes institucionales (Celorio, 2016).

La desposesión de DH es su cancelación de facto; sin embargo, es importante analizar que esta cancelación no es equivalente a una derogación, suspensión, revocación o anulación de DH porque, justamente, lo que define y construye al Estado moderno son los DH. El sistema político basado en la democracia exige un Estado de Derecho en alianza con los DH, de ahí que ni en términos de acción gubernamental ni en términos de discurso, el aparato estatal puede derogar los DH en las democracias contemporáneas.

Frente a la cancelación de facto de DH, la categoría analítica que propongo es desposesión de DH, que se opera a la par de la violación, pero también a la par de la defensa y la promoción. Es decir, la realidad sociopolítica es tan compleja que al mismo tiempo confluyen la violación, la desposesión y la defensa de DH.

Si hablamos de desposesión no hay defensa porque no hay violación; no hay reparación del daño porque no hay violación y los discursos de exigibilidad pierden fuerza frente a la tiranía de leyes que opera ajustes institucionales basados en el Derecho positivo, es decir, en el conjunto de normas vigentes en un momento dado que deben aplicarse. Frente a la desposesión legal de DH quedan normalizados regímenes de excepción y condiciones de vulnerabilidad, precariedad e inseguridad.

Respecto a internet, la desposesión de DH consiste en ajustar leyes para permitir la videovigilancia, el espionaje electrónico y la censura en internet. No menos importante es permitir el uso de *cookies* y *web bugs* para sustraer información y construir perfiles de *big data* para hacer de este territorio digital un centro comercial 24 por 7, que tenga segmentación de mercados y perfiles de consumidores, sin invertir en estudios de mercadeo.

Mientas que la desposesión ocurre a partir de leyes que permitan reconfigurar el territorio digital, para usufructuarlo con fines de vigilancia, control, acumulación de la riqueza y censura, la violación de DH en internet, si bien tiene los mismos fines arriba mencionados, transgrede la ley; en ambos casos se producen estados de excepción digital que se operan a partir de una racionalidad gubernamental biopolítica.

En cuanto al actor que desposee DH, en términos de ajustes institucionales vía promulgación de leyes, queda claro que es aparato estatal. Sin embargo, como apunté arriba, estos ajustes institucionales que explica Harvey son para la reconfiguración territorial y son producto, en parte, de negociaciones pugnadas por el capital.

En este marco, si se reconociera al capital como actor no estatal que desposee DH, desposeería derechos de intimidad, libertad de expresión, libertad de tránsito. Si no se reconoce como tal y se queda la noción de que es el aparato estatal quien desposee estos derechos, la cuestión que urge es que el capital está operando como una fuerza parapolicial que opera la desposesión de derechos. Es decir, está haciendo tareas que, para efectos de impugnación de violación de DH, le corresponderían al aparato policial; cuando el Estado viola DH por acción lo hace a través de sus agentes policiacos y militares. Pero, en el caso de que el Estado desposee DH en Internet, a veces lo operan agentes estatales, a veces agentes no estatales que trabajan en la multinacional.

Usuarios de internet en México

Cifras oficiales establecen que la penetración de internet en México alcanza 59.8% de la población, lo que equivale a 65 millones de internautas, de los cuales 77% se conecta a la red mediante un Smartphone (AMPICI, 2016).

Si bien el número de mexicanos y mexicanas conectados a internet se ha incrementado de manera significativa durante los últimos 10 años, las cifras que da a conocer la Asociación Mexicana de Internet a través de su Estudio Usos y Perfiles de Internet en México 2016 y que ratifica el INEGI me parecen excesivas.

Ni el INEGI ni la AMPICI explican la metodología a través de la cual concluyeron que casi 60% de mexicanos están conectados a internet[5]. Si contaron el número de usuarios conectados a una dirección IP o que contrataron un servicio de datos en una empresa de telefonía, se corre el riesgo de haber contar por dos o tres a un mismo usuario. Es decir, si una persona tiene un punto de red en su oficina, tiene contratada en casa una conexión de red inalámbrica y además también tiene contratado un paquete de prepago de telefonía y datos, esta persona tiene tres cuentas de internet, pero en realidad es sólo un usuario y no se puede contar por tres usuarios. Esto podría significar la reducción a la mitad del número de usuarios contabilizados, es decir, podría ser que en realidad en México de 30% a 40% de la población tiene acceso a internet y no 60% como se informa a través de cifras oficiales[6].

Según la Unión Internacional de Telecomunicaciones y el Banco Mundial, en 2014, en México, 44 % de la población tenía acceso a internet y, en el año 2000, 5.1% de la población estaba conectada (UIT-Banco Mundial, 2014).

Sin lugar a dudas, estas cifras reflejan el enorme esfuerzo que capitales nacionales y multinacionales, junto con gobierno federal, han realizado para ampliar la cobertura y el acceso a internet. No obstante, habría que cuestionar estas cifras, pues a simple vista resultan improbables, sobre todo si consideramos el informe de la CEPAL donde señala que "México es uno de los tres países, junto con Guatemala y Venezuela, en donde más ha crecido la pobreza. Entre 2014 y 2015, […] la pobreza en México avanzó de 51.6% de la población del país en 2012 a 53.2% en 2014" (Gazcón, 2016). Para ese año, el INEGI contó 119 millones 530 mil 753 mexicanos (INEGI, 2015).

Si cotejamos con los niveles de pobreza que marca la CEPAL, significa que en México existían 63 millones de personas en pobreza y en pobreza extrema, mientras que AMPICI asegura que alrededor de 65 millones mexicanos tiene acceso a internet[7].

Este tratamiento de la información en relación con el acceso a internet en México es significativo en el marco de la reciente declaración de la Organización de Naciones Unidas que reconoce internet como un derecho humano. En junio de 2011, "La Asamblea General de la Organización de las Naciones Unidas (ONU) ha declarado el acceso a internet como derecho humano altamente protegido. La ONU exige a los países miembros facilitar un servicio accesible y asequible para todos y estima como una prioridad asegurar a la ciudadanía el acceso a internet" (Helphone, 2011).

Sea de una forma u otra, 65 millones de usuarios (AMPICI e INEGI) o entre 30 y 40 millones de usuarios, es un hecho que la brecha digital no se ha abatido y que el Estado mexicano viola por omisión el derecho humano a internet a por lo menos 50 millones de personas: con ello se limita el desarrollo, la libertad de expresión y opinión, el acceso a la información y al conocimiento, la difusión de la cultura, entre otros.

La brecha digital puede definirse como la distancia que existe entre la población con acceso a internet y la población sin acceso. Esto significa que internet también ha operado como un factor que produce desigualdad social, considerando los efectos que ésta produce en la sociedad basada en competencias.

Por otra parte, en relación con identificar cómo internet ha transformado comportamientos individuales y sociales en México, cabe señalar que, según la AMPICI, la interacción en redes sociales, jugar en línea y ver películas y series vía *streaming*[8], son las tres preferencias principales que las y los usuarios de internet tienen para efectos de diversión y ocio.

Así, Facebook es la red social líder en México, con 60 millones de cuentas, le siguen aplicaciones como Whats App[9], YouTube, Linkedin y Twitter.

Según la revista *Merca2.0*, Facebook en México cuenta con más de 60 millones de usuarios de entre 13 a 65 años, de los cuales 6.9 millones son menores de entre 13 y 17

[5] A 80% de los de los usuarios les interesa tener acceso a redes sociales y las principales barreras que encuentran es que la conexión a internet es lenta.

[6] Es importante señalar que la Unión Internacional de Telecomunicaciones y el Banco Mundial manejan las mismas cifras, pues basan sus publicaciones en datos ofrecidos por el INEGI.

[7] Esto no significa que las personas pobres no tengan acceso a internet, sino que no la totalidad de las personas pobres tiene acceso a internet.

[8] Término que hace referencia a poder ver películas y escuchar música sin necesidad de descargar los archivos; práctica que incrementa el consumo de megas.

[9] Cabe mencionar que Facebook compró Whats App y que próximamente este servicio de mensajería por internet entregará a Facebook los números telefónicos de sus usuarios.

años; Ecatepec es la población mexicana con la mayor cantidad de usuarios, 16 millones; México es el décimo país en cuanto a número de usuarios en el mundo y en su buscador se realizan en promedio mil quinientos millones de búsquedas al día.

Algo similar ocurre con la cantidad de cuentas activas de Facebook. Un usuario puede tener entre dos y tres cuentas, y eso significaría que, en México, alrededor de 20 o 30 millones de usuarios estarían gestionando las 60 millones de cuentas activas que reporta Facebook.

Las razones por las que un usuario puede tener más de una cuenta pueden ser, por ejemplo, que los maestros tienen su cuenta personal y abren otras para actividades de aprendizaje complementarias vía Facebook, profesionistas que abren sus cuentas para interactuar con su medio profesional y su ámbito personal, activistas de DH y líderes de organizaciones civiles, sindicatos y movimientos sociales que tienen sus cuentas personales y sus cuentas profesionales, y del mismo modo funcionarios públicos, legisladores, políticos, celebridades, etcétera.

No obstante lo anterior, Facebook es la red social con mayor penetración en México. De ahí el interés por interceptarlo para espiar las comunicaciones electrónicas que publican las y los usuarios.

Violación y desposesión de DH en internet

En términos generales, los DH que se violan y se desposeen en internet son: derecho a la intimidad, a la privacidad, a la protección de datos, a la libertad de expresión, al libre acceso a internet y en términos sólo de violación por omisión al acceso a internet.

El espionaje electrónico y la videovigilancia son dos actividades que gobiernos y capitales realizan actualmente de manera cotidiana a través de internet, tanto en México como en muchos países del mundo. En ambos casos, se puede hablar de que son prácticas que se operan tanto de manera legal como ilegal; sin embargo, el hecho de que sean prácticas legales no les confiere legitimidad, pues requieren mecanismos de transparencia que puedan dar cuenta de cómo se opera y qué se hace con la información recabada, situación lejana en México.

Lo que sí es una realidad es que en ambos casos, el ilegal y el legal, se vulneran DH. A continuación analizo estas prácticas en términos de violación y desposesión de DH.

Espionaje electrónico: violación de DH

El espionaje ilegal: violación de DH

El espionaje electrónico es aquella actividad secreta y encubierta realizada por intrusos, sean programas de software o hackers, que violan los sistemas de seguridad de sitios y aplicaciones de internet, que entran sin permiso para consultar información y crear perfiles de asociación, de navegación y de movilización social. Estos sitios y aplicaciones pueden ser privados; es decir, pertenecer a individuos, organizaciones civiles, movimientos sociales, iglesias, comercios, bancos, etc., o públicos como sitios de gobiernos, legislaturas, partidos políticos, etc. Aquí lo privado tiene que ver con la distinción entre la esfera pública gubernamental y la esfera privada no gubernamental, y no tiene relación con lo confidencial, pues en ambos casos la información es confidencial.

Como actividad clandestina es ilegal[10] y viola el derecho a la intimidad al cancelar la privacidad de las personas, pues las coloca en estado de fragilidad, por lo que pueden ser víctimas de otras violaciones como persecución, desaparición forzada, tortura, censura, etcétera.

El artículo 12 de la Declaración Universal de Derechos Humanos de la ONU, firmada y ratificada por México, 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" (ONU, 1948).

En contraste:

> El Ejército Mexicano, que legalmente no está facultado para intervenir comunicaciones privadas, negoció este año un contrato millonario con la empresa de ciber espionaje Hacking Team para la compra de una versión especial de su software Galileo que tiene la capacidad de infectar las computadoras y celulares de hasta 600 blancos distintos y robar toda su información. […] la Sedena pidió que el monitoreo remoto (espionaje) pudiera hacerse mediante un ataque que se transmitiera con imágenes, mensajes de texto o incluso los llamados códigos QR (Ángel, 2015).

[10] Hago esta aclaración porque existen legislaciones específicas que legalizan el espionaje electrónico y es cuando hablo en términos de desposesión de derechos humanos.

Espían redes sociales

> La empresa Hacking Team tiene entre sus clientes predilectos en el mundo a la Secretaría de Gobernación de México, a la que le dio descuentos de cientos de miles de pesos para renovar los programas de intrusión junto con un software especial que puede atacar múltiples objetivos e intervenir redes como Facebook, Twitter y Gmail[11]. Entre las mejoras del software está el módulo *Inteligence* para intervenir redes sociales. Hacking Team le ha facturado a Gobernación entre 2010 y 2015, más de 24 millones de pesos. […] De las 35 naciones en el historial de clientes de la firma italiana, México es el país que ha facturado la mayor cantidad de dinero, y de la cartera de 16 compradores mexicanos el que más ha pagado es la Secretaría de Gobernación, Pemex, la Policía Federal, la Secretaría de Marina y el Cuerpo de Seguridad Auxiliar del Estado de México (Ángel, 2015).

Espionaje electrónico: desposesión de DH

El espionaje legal: desposesión de DH

La geolocalización y monitoreo de llamadas y comunicaciones electrónicas en smartphones, y el espionaje electrónico reglamentado en el Acta Patriota de Estados Unidos, el uso de *cookies* y *web bugs*, y el derecho al olvido son cinco ejemplos.

Geolocalización de personas en tiempo real sin autorización judicial

La Suprema Corte de Justicia de la Nación avaló el artículo 190[12] del Título Octavo sobre la colaboración con la justicia de la Ley Federal de Telecomunicaciones y Radiodifusión reformada en junio de 2016 donde autoriza el monitoreo en tiempo real para localizar y ubicar a un usuario a través de su teléfono móvil sin previa autorización judicial e intervenir comunicaciones electrónicas.

Esta sentencia implica la desposesión del derecho a la intimidad, a la privacidad y al debido proceso. Sobre todo en un país donde el Estado de Derecho está en crisis.

El argumento central de la SCJN es que no se interfiere con el derecho a la privacidad de la persona porque "no se *geolocaliza* a una persona, sino a un teléfono (conectado a internet)". Una lógica verdaderamente risible. Es claro que los datos de localización de un teléfono, tanto históricos como en tiempo real, se encuentran asociados a una persona identificada o identificable; pero, más aún, localizar un teléfono le da acceso a la autoridad de todos los datos confidenciales que en él se almacenan. Al observar los lineamientos emitidos por el Ifetel, así como el manual de procedimientos de la PGR para la gestión de la geolocalización, dejan claro que se trata de un monitoreo continuo de un "objetivo" con la intención de analizar sus patrones de conducta (y sus comunicaciones). Los usuarios de smartphones[13] están en riesgo de ser monitoreados "legalmente" por autoridades sin que exista ningún mecanismo de rendición de cuentas ni previa autorización judicial, lo que también desposee el derecho a un juicio justo (R3D.mx, 2106).

Intervención legal de comunicaciones electrónicas privadas

El derecho a la intimidad y a la privacidad está condicionado en Ley de Telecomunicaciones y Radiodifusión, pues legaliza la intervención de comunicaciones electrónicas privadas sin consentimiento ni conocimiento de quienes las emiten y reciben. El último acápite del artículo 190 de dicha ley dice: "Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal o el titular del Ministerio Público de la entidad federativa correspondiente podrá autorizar la intervención de cualquier comunicación privada" (publicada en 2014 y reformada en 2016).

[11] *Animal Político* ubicó un contrato clasificado como "estrictamente confidencial" en el que el CEO de la firma italiana, Valeriano Bedeschi, le explica a Gobernación cómo funciona el programa espía Da Vinci.

[12] "La Ley Federal de Telecomunicaciones y Radiodifusión obliga a las empresas de telecomunicaciones a retener los metadatos de las comunicaciones de todos sus clientes por un lapso de 24 meses. Éstos incluyen origen, destino, duración, fecha, hora y ubicación de las comunicaciones. Se ha demostrado que pueden ser utilizados para revelar aspectos sensibles sobre la vida privada de las personas. La SCJN declaró constitucional el artículo 190, permitiéndoles a ciertas autoridades, previa autorización judicial, el acceso a estos metadatos, y los usuarios no tienen derecho a acceder sus propias comunicaciones".

[13] Al cierre del primer trimestre de este año, 73.4% del total de líneas móviles en México correspondían a smartphones, lo que suma un total de 79.98 millones de dispositivos, señala la consultoría The Competitive Intelligence Unit (CIU) (la.cronica.mx, 2016).

Este último párrafo desposee el derecho a la intimidad, a la privacidad, a la confidencialidad, a un juicio justo y a un debido proceso a todos los mexicanos que mantengan un medio de comunicación electrónico, sea WhatsApp, mensajería instantánea como Messenger, el chat de Facebook, el correo electrónico, etcétera.

Por simple interés de la autoridad judicial o ministerial, legalmente se pueden intervenir comunicaciones electrónicas sin justificar el motivo de la intervención. Suelen ser de máximo interés las comunicaciones que entablan periodistas con sus fuentes, activistas y defensores de DH con sus homólogos, sindicalistas, estudiantes, ambientalistas, etc. Aunque, en el discurso oficial sobre intrusiones en las comunicaciones privadas, las narrativas van en el sentido de proteger a la sociedad del narcotráfico, del crimen y la delincuencia común; no obstante, la política de seguridad nacional cataloga como amenazas a los movimientos sociales, motivo que hace pensar que la geolocalización y el espionaje electrónico también tienen estos objetivos.

USA Patriot Act, acta patriota

El gobierno de Estados Unidos, bajo la administración Bush, promovió la aprobación de la *USA Patriot Act* en 2001, se reautorizó en 2006 y 2015 (Obama). Legaliza la vigilancia y espionaje electrónico de la población civil, sin previa orden judicial. Ahora directamente agentes de la CIA, el FBI, la NSA, la Interpol y de las agencias de inteligencia y policías locales del mundo están legalmente autorizados para espiar a los ciudadanos de casi todo mundo; esta ley tiene un aspecto realmente crítico debido a la ambigüedad en la definición de terrorismo/terrorista y criminal/criminalidad; al criminalizar la inmigración hacia Estados Unidos, por ejemplo, el gobierno de este país puede elevar y, de hecho ya lo hace, a categoría de criminal al (in)migrante y, en consecuencia, criminalizar los movimientos sociales de derechos humanos que se movilizan para defenderlos. El tercer aspecto critico también se refiere a su carácter extraterritorial, ya que abarca jurisdicción internacional y se apoya en los tratados internacionales y convenios bilaterales (y en la excepcionalidad extraterritorial de Estados Unidos que se permite acciones fuera de sus fronteras geográficas) su cumplimiento es obligatorio para toda entidad que quiera hacer negocios con Estados Unidos y los países miembros de la ONU.

Con esta ley se obliga a todas las entidades bancarias y financieras del mundo interesadas en tener relaciones comerciales y de negocios internacionales con algún banco o entidad financiera de Estados Unidos a entregar información sobre la naturaleza de sus negocios y sus clientes (Celorio, 2011).

¿Legalización de la censura?

Derecho al olvido es el nombre que refiere al derecho de cualquier usuario o usuaria de internet a que la información que se publica sobre él o ella en sitios web y que luego la hagan disponible los motores de búsqueda sea borrada de internet. Pareciera que protege la privacidad, la reputación y la identidad de las personas y está relacionado con los derechos ARCO[14] (Acceso, Rectificación, Cancelación y Oposición). Sin embargo, este es un derecho del ámbito personal a través del cual se puede cancelar el derecho a la libertad de expresión y obstruir la libertad de navegación, de información y de consulta. En México se ha utilizado como una práctica de censura.

En México, este debate comenzó en 2015, cuando el Instituto Nacional de Acceso a la Información (INAI) anunció un proceso sancionador contra Google México porque un ciudadano no había podido ejercer su derecho a cancelar sus datos personales en internet.

El caso fue promovido por el empresario Carlos Sánchez de la Peña, quien pidió a Google que eliminara varios resultados de búsqueda relacionados con su nombre. Uno de esos enlaces llevaba al reportaje periodístico "Fraude en Estrella Blanca alcanza a Vamos México", publicado en 2007 por la revista *Fortuna*. En esta nota, el empresario está implicado en presuntos actos de corrupción.

Ante la negativa de Google de retirar los enlaces, Sánchez de la Peña inició un procedimiento de protección de derechos ante el INAI alegando que la nota afecta a su esfera "más íntima" y también a sus "relaciones financieras actuales". El Instituto ordenó a Google que removiera los enlaces, basado en el derecho al olvido. "[…] Eliminalia, es una empresa […] dedicada a borrar su pasado, porque usted también tiene derecho al olvido". Dídac Sánchez, el fundador de esta compañía, dijo que tiene alrededor de 400 clientes mensuales entre políticos, personas de negocios, ciudadanos.

[14] Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) son un conjunto de derechos que garantizan al ciudadano el poder de control de sus datos personales. Lo más importante en el ejercicio de este derecho es que sólo el titular de los datos personales puede solicitar el acceso, la rectificación, cancelación u oposición, siempre que se encuentren en un sistema de datos personales. Por tanto, en este tipo de solicitudes es indispensable que sea acreditada la personalidad del solicitante o bien la del representante legal (Gobierno de la Ciudad de México, 2016).

Un grupo heterogéneo de clientes que paga cifras que van desde los 3 mil euros "si eres un ciudadano anónimo" (60 mil pesos aproximadamente), hasta los 20-30 mil euros "si eres un personaje público" (400-600 mil pesos), o incluso hasta los 100 mil "si eres un personaje muy público" (2 millones de pesos) (Ureste, 2016).

Con la ley sobre el derecho al olvido se corre el riesgo de desposeer el derecho a la información, que es un bien público y un derecho humano; se ofrecen mecanismos para que el sector privado comercialice la censura y saque de la indexación de los motores de búsqueda información referente a acciones de agentes de gobiernos, empresas y ciudadanos, lo cual puede ser una suerte de legalización de la censura.

Cookies y *web bugs*, herramientas que violan la privacidad en internet

Desde una óptica de DH en la que no sólo el agente estatal viola DH sino también otros actores, en este caso el capital, las *cookies* y los *web bugs* operan como herramientas que le ofrecen al sector empresarial, gubernamental y civil los mecanismos informáticos para conocer el comportamiento de navegación de los y las usuarias de internet, recolectar información confidencial y construir perfiles de usuarios y consumidores, con lo que pueden segmentar de manera exitosa sus mercados mediante anuncios publicitarios acoplados a los intereses y comportamientos de las y los usuarios que previamente vigilaron. Después entran sin permiso a sus espacios digitales, personales y confidenciales como son el correo electrónico, las redes sociales y los motores de búsqueda que publican productos y servicios que fueron consultados en tiendas en internet como Dealextreme, E.bay o Mercado Libre; empresas que legalmente no pueden publicar sus productos porque los comportamientos de navegación que se les compartieron violaron derechos humanos y contravinieron legislaciones nacionales como aquellas plasmadas en el Código Civil Federal y en la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Para fundamentar lo anterior, primero explicaré qué son y cómo operan las *cookies* y los *web bugs*, para después analizar qué derechos humanos se violan y desposeen y qué artículos de las leyes citadas se infringen.

Las *cookies* son archivos de texto que recopilan y almacenan información para dar un seguimiento de la navegación de un usuario en internet. Existen diferentes clases de *cookies*: *session cookies*, con un tiempo corto de vida pues se borran al cerrar el navegador; *persistent cookies*, escudriñan el comportamiento de la y el usuario en virtud de que guardan su información en un sitio o servidor web; *zombie cookies,* son archivos que se autogeneran nuevamente después de que los borran, lo cual significa que el navegador no tiene ningún poder sobre ellas porque continuarán regenerándose. Las *cookies zombis* se guardan en el dispositivo y no en el navegador para tener acceso a éstas sin importar qué navegador se use. Esto invade la propiedad privada de los y las usuarias. "Esta misma característica puede convertirlas en una amenaza para la privacidad y seguridad del usuario" (González, 2014).

Por lo general, cuando aceptamos el uso de *cookies*, la administración del sitio en cuestión no aclara el tipo de *cookies* a las que hacen referencia cuando solicitan su aceptación. Existen tres tipos de aviso de uso *cookies* en internet:

1. Los sitios que notifican: "Este sitio usa *cookies* para mejorar su experiencia. Si continúa en el mismo, consideramos que acepta su uso", pero no trae el aviso de privacidad ni el contrato de consentimiento y es acto coercitivo que condiciona la navegación.
2. Los sitios que dicen: "Este sitio web utiliza *cookies* para que usted tenga la mejor experiencia de usuario. Si continúa navegando da su consentimiento para su aceptación, Para consultar la *política de cookies*, siga este hipervínculo". La primera parte es una publicidad engañosa porque las *cookies* nos son para que el usuario tenga una mejor experiencia de navegación y este tipo de publicidad está prohibida. Al dar *click* en el hipervínculo no existe ningún documento, lo cual es ilegal por dos razones: existe omisión en el contrato de consentimiento y la Ley Federal de Protección de Datos Personales en Posesión de Particulares exige que debe estar visible el contrato o aviso de privacidad para no violar el derecho a la privacidad.
3. Los sitios que informan con más ética que usan "*cookies* propias y de terceros para mejorar sus servicios, para análisis estadístico y para mostrar publicidad: "Si continúa navegando consideramos que acepta su uso en los términos establecidos en la *Política de cookies*". Al consultar la política de *cookies* expresan la entrega terceros[15]. Sin embargo, como explico más adelante, esto viola el derecho a la intimidad y a la privacidad.

[15] A continuación se detallan las entidades distintas al titular que utilizan *cookies* en el sitio web, así como las finalidades de las mismas:

En los tres casos señalados, en principio el aviso de uso de *cookies* viola de manera indubitable el Código Civil Federal y convierte en ilegal esta práctica, por lo que se viola el derecho a la privacidad. El artículo 7 establece que "la renuncia autorizada en el artículo anterior no produce efecto alguno si no se hace en términos claros y precisos, de tal suerte que no quede duda del derecho al que se renuncia". Cuando el o la usuaria del internet acepta el uso de *cookies*, no queda ampliamente explicado que está renunciando a su derecho a la privacidad, por lo que el aviso de privacidad no puede surtir efecto y, en consecuencia, es ilegal recolectar y compartir información de los y las usuarias de internet. En este sentido, el gobierno mexicano viola por omisión dicho derecho y desposee por omisión los derechos que de éste se desprenden.

Ahora, el artículo 6° del mismo Código Federal establece que la voluntad de los particulares no puede eximir de la observancia de la ley ni alterarla o modificarla. Sólo pueden renunciarse los derechos privados que no afecten directamente al interés público, cuando la renuncia no perjudique derechos de terceros (2013).

Para efectos de este trabajo, dicho artículo encierra una doble interpretación: 1) sólo pueden renunciarse los derechos privados que no afecten directamente al interés público. Con este artículo se deja paso libre a que en el aviso de *cookies* se renuncie al derecho privado ya que no afecta a terceros. Sin embargo, este ordenamiento legal, que de ninguna manera es menor, es decir es el Código Civil Federal, abre un resquicio para una renuncia de derechos privados. En este caso, el derecho a la privacidad no es un derecho privado, es un derecho humano que emana del derecho a la confidencialidad que mencioné al principio, pero que vale la pena recordar. El artículo 12 señala: "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". Y, en este caso, con el uso generalizado de *cookies* existe una desposesión del derecho humano a la confidencialidad.

2. Si recuperamos la primera parte de este artículo 6°: la voluntad de los particulares no puede eximir de la observancia de la ley, ni alterarla o modificarla; lo que indubitablemente significaría que este acuerdo entre particulares respecto a la aceptación de la vigilancia y el espionaje vía *cookies* es improcedente y, por ende, es ilegal.

Por otro lado, según el IFAI, el aviso de privacidad debe contener ciertos elementos que indiquen que en ninguno de los tres casos descritos el uso de las *cookies* en internet es legal.

Respecto al primer caso, no tiene aviso de privacidad; el segundo caso tiene un hipervínculo que no lleva a ninguna parte, por lo que se infringe, por inexistencia del contrato, el principio de información que establece la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; respecto al tercer caso que sí ofrece el aviso de privacidad, éste no especifica cómo obtiene los datos personales y no identifica quién es el responsable del uso de los datos personales.

La publicidad[16] como dispositivo que viola DH en internet

En principio, el descomunal uso de la publicidad en internet viola el libre acceso a la información y el libre tránsito por internet; la publicidad generada vía *cookies* viola el derecho a la intimidad, la privacidad y la confidencialidad de datos, permite el robo y venta de información de las y los usuarios de internet, y profundiza la desigualdad social mediante el sistema de indexación de Google, que primero despliega los enlaces de los sitios que pagan publicidad.

cookies de redes sociales: el titular utiliza *cookies* de Facebook, Twitter y Google Plus para que el usuario pueda compartir contenidos de la web en las citadas redes sociales, o bien para facilitar el registro en la web, de forma que con los datos que los usuarios han facilitado las redes sociales puedan cumplimentar directamente los campos del formulario de registro en la web. *Cookies* para la medición del tráfico en los portales: el titular utiliza *cookies* de Google Analitycs y Certifica Metric para recopilar datos estadísticos de la actividad de los usuarios en el sitio web y, de este modo, poder mejorar los servicios prestados a los usuarios. Estas *cookies* permiten analizar el tráfico de usuarios generando un ID de usuario anónimo que se utiliza para medir cuántas veces visita el sitio un usuario determinado. Asimismo, registra cuándo fue la primera y última vez que visitó la web, cuándo se ha terminado una sesión y el origen del usuario. *Cookies* con finalidad publicitaria: Google Adsense y Dobleclick insertan *cookies* a los usuarios de la web para mostrarles contenidos publicitarios afines a los mismos, basándose en las interacciones previas de los usuarios, las visitas al sitio web del anunciante, IP de origen, etc. De este modo, con los datos que se recopilan a partir de las *cookies*, los anuncios mostrados en el sitio web se publican y administran más eficientemente.

[16] Una piedra angular que sostiene al capitalismo contemporáneo es, sin lugar a dudas, la publicidad en tanto que es el mecanismo que acerca los procesos de producción con los de consumo; reduce el tiempo entre la producción de la mercancía y su exposición en los escaparates y puntos de venta. A través de su discurso multimedia ofrece, en diversas plataformas tecnológicas, retóricas de felicidad y plenitud que, al tiempo de recuperar la ideología dominante y reproducir las condiciones de producción, recrea necesidades y aspiraciones.

Con internet la publicidad se transformó completamente; se hizo más fuerte y logró su meta más añeja: segmentar mercados y llegar al consumidor real, hizo de internet un territorio mediado por el capital, basado en el consumo. Los mercadólogos y publicistas espían el comportamiento de las y los usuarios, sus preferencias, perfiles e historias de navegación. El concepto de espiar tiene una connotación de intrusión y de ilegalidad. Sin embargo, como se están utilizando, los avisos de *cookies* son una práctica que si bien infringe la ley, se encuentra normalizada.

Según la AMIPCI, "el comercio electrónico tiene un valor de 164 mil millones de pesos. El crecimiento del 2013 a 2014 fue de un 35 %; las pequeñas y medianas empresas representan el 76% del mercado de comercio electrónico por tamaño de negocio. […] Los adultos entre 18 y 34 años encabezan la tendencia con un 88% de compradores vía teléfonos inteligentes, PayPal tiene una participación del 61% en el procesamiento de pagos" (Baéz, 2015).

El libre acceso a la información

Los anuncios publicitarios en internet consumen, sin autorización de las y los usuarios, datos en internet, es decir, ancho de banda; además de estar obligados a ver y escuchar anuncios publicitarios no solicitados que requieren mucho tiempo de descarga y de dispositivos robustos para que se desplieguen los anuncios. ¿Por qué se considera mala práctica al *spam* que es correo no solicitado y fundamentalmente correo publicitario mientras que la publicidad no solicitada no está considerada como mala práctica o delito en internet?

La publicidad viola *el libre tránsito por internet*: cuando un automovilista circula por calles y carreteras y se colocan retenes sanitarios, policiacos y militares, se está obstaculizando la movilidad; cuando más de 50% de la pantalla es publicidad colocada vía información obtenida por *cookies* y *web bugs*, también aleatoriamente, considero que se obstaculiza la navegación, tanto en capacidad de descarga como de lectura, sin retenes publicitarios. Pero la publicidad es sólo una actividad, pues quien violenta los derechos es el capital y el Estado.

Por otro lado, así como internet transformó sustancialmente la publicidad en los últimos 10 años, segmentándola por la misma información que ofrecen los usuarios y ahorrándoles a los fabricantes los estudios de mercados, de preferencias y de hábitos, la publicidad transformó internet en un centro comercial. La oferta llega a tal punto que por más megas de internet que se tengan contratadas, la velocidad de descarga se vuelve lenta y la experiencia de navegación horrorosa. Ahora Hotmail ofrece un paquete de menos de 10 dólares al año para no colocar su banner de publicidad en el lector de correo electrónico.

La publicidad ha convertido a la mayoría de los sitios de internet en un escaparate publicitario que llega a tal extremo de vulnerar el acceso al conocimiento y a la información, ahogando a los y las usuarias en un enorme mar de anuncios.

Videovigilancia, desposesión del derecho a la intimidad

La videovigilancia es una práctica que se opera de manera legal e ilegal. Al ser legal, desposee el derecho a la intimidad. Si bien es una práctica que se extiende cada vez más en el país, en este apartado refiero unos ejemplos para confrontarlos con el análisis de violación y desposesión de DH en México.

Bajo la promesa de ciudades seguras la ciudadanía cede su derecho a la intimidad frente al miedo a la violencia, y renuncia a este derecho sin conocimiento real de lo que está cediendo; además, tampoco es transparente la información de los tres niveles de gobierno a lo largo del país sobre cómo se opera la videovigilancia, qué hacen con la información almacenada y acerca del riesgo que existe de que esta información pueda ser *hackeada*, es decir, colocaría en manos de terceros información sensible de las personas.

¿Ciudad segura?

La Ciudad de México, según *El Financiero*, es una de las ciudades más videovigiladas del planeta. A través del programa Ciudad Segura, que inició en 2009, se han instalado, a la fecha, más de 14 mil videocámaras, y la meta es llegar a 20 mil dispositivos en 2017. Entre los aspectos que vigilan son zonas rurales, unidades habitacionales y reconocimiento de placas. Toda la información se analiza desde el C4, conocido como El Bunker, donde el gobierno de la ciudad tiene acceso a todos los videos de la metrópoli (*El Financiero*, video).

Homologación de la videovigilancia en México

La Secretaría de Gobernación, a través del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP), presentó la norma técnica para estandarizar las caracte-

rísticas técnicas y de interoperabilidad de los sistemas de videovigilancia de seguridad pública del país, cuyo objetivo es ordenar los criterios del uso del Fondo de Aportación para la Seguridad Pública (FASP) y del subsidio para el Fortalecimiento de la Seguridad en los municipios (Fortaseg) del año en curso (Secretaría de Gobernación, 2016).

Ley que no considera intromisión a la privacidad a la videovigilancia

El Congreso del Estado aprobó la Ley que Establece las Bases para la Videovigilancia en el Estado de Durango; su precursor, "Rodolfo Guerrero García, señala que el Artículo 7 fracción XII define la videovigilancia como la captación de imágenes con o sin sonido por los cuerpos de seguridad pública estatal, municipales, de seguridad privada, o particulares, que realicen en términos de la presente ley". La ley deja claro que "No se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y/o familiar y a la propia imagen, las grabaciones obtenidas en cumplimiento de mandato de autoridad jurisdiccional federal o local previamente emitida con la debida motivación" (Madera, 2012).

Esta es la mejor muestra de cómo se desposee el derecho a la intimidad mediante una ley de orden local, contraviniendo los artículos 6 y 7 del Código Civil Federal y el artículo 12 de la declaración que ya fueron analizados.

Conclusiones

A lo largo del texto corroboramos que la violación y desposesión de DH en internet es una realidad intangible que muchas veces pasa desapercibida entre los y las usuarias. Los derechos que más se vulneran por las dos vías son: el acceso a internet, y con éste el acceso a la información y al conocimiento; el derecho a la intimidad, a la privacidad, a la protección de datos, lo que implica riesgos también en relación con quién y dónde se almacenan estos datos. Además, del riesgo que implica para los y las usuarias de internet ser vigilado y espiado por agentes privados o del gobierno y que se incrementa cuando los datos son almacenados. La libertad de expresión, y con ello la seguridad de activistas, periodistas y defensores de DH, también es un derecho que se viola y se desposee.

Por otro lado, requerimos de un esfuerzo epistemológico para poder identificar lo que está sucediendo en y con internet y problematizarlo a la luz de los DH y, en este sentido, lograr categorizar, definir, ampliar, adaptar y proponer nuevas formas de explicarnos la realidad. La conceptualización en relación con la violación de DH y con la categorización de DH ya no alcanza para nombrar las cosas que suceden, ni tampoco son suficientes para protegernos. Requerimos reivindicar y construir nuevos derechos en internet, los cuales ya están plasmados en la Carta Internacional de Derechos Humanos y Principios de Internet, pero aún no son DH.

Si bien el concepto de desposesión de DH que propongo puede ser controversial, pues aparentemente no se pueden sustraer derechos, en la vida real, en la praxis y *de facto* sí sucede. Sólo si logramos nombrar la realidad como es, podremos comprenderla y modificarla.

Por otro lado, la publicidad devasta internet y los DH aquí explicados. Esto es un espejo y, como el capitalismo contemporáneo está reconfigurando el espacio público y el medio ambiente mediante el despojo y la desposesión, también ha reconfigurado en los últimos tres años el espacio digital.

Quedó claro que los DH deben estar protegidos tanto dentro como fuera de internet; es decir, no hay DH que apliquen para entornos digitales y derechos humanos que apliquen en entornos materiales. Sin embargo, están sucediendo cosas en internet que requieren una reflexión crítica cuya mirada vea los DH; un ejemplo es la fragilidad de México y de los mexicanos en materia de ciberseguridad; el país no tiene una política de Estado, una visión de Estado sobre las vulnerabilidades en seguridad informática.

> México está rezagado en seguridad cibernética. Tal atraso deja vulnerable la información de los usuarios, los datos gubernamentales y de empresas, así como infraestructura crítica del país. La OEA indica que las naciones más afectadas por delitos informáticos son Brasil, México y Colombia. […] El Índice mundial de ciberseguridad elaborado por ABI Research y la Unión Internacional de las Telecomunicaciones (UIT) exhibe las debilidades de la ciberseguridad mexicana: señala que se carece de un marco de ciberseguridad para la certificación y acreditación de agencias nacionales y profesionales en el sector público y de un mapa de ruta nacional de gobernanza para el tema (Godoy, 2015).

Finalmente, vale la pena reflexionar sobre la obsolescencia tecnológica y los DH que se violan y desposeen y aquellos que debieran construirse alrededor de ésta. De acuerdo con el Instituto Nacional de Ecología y Cambio Climático, "México genera alrededor de 350 mil toneladas

de residuos eléctricos y electrónicos cada año[17]. La obsolescencia hace que las cosas dejen de servir antes de que se descompongan, aunada a los sistemas de licencias, los sistemas operativos y el desarrollo de virus.

Referencias

Agamben, G. (2007). *Estado de excepción*. Buenos Aires, Argentina: Adriana Hidalgo Editora.

AMPICI (2016). *Estudios sobre los hábitos de los usuarios de Internet en México 2016*. Asociación Mexicana de Internet.

Ángel, A. (2015). "Sedena negoció compra de software a Hacking Team en 2015 para espiar a 600 personas", *Animal Politico* (Seguridad).

Baéz, J. (2015). "El comercio electrónico en México en 10 datos". *Dinero en Imagen*.

Celorio, M. (2016). "Desposesión de derechos humanos en el capitalismo contemporáneo", en Estévez, Ariadna, y Vázquez, Daniel, *El capitalismo neoliberal y sus descontentos: 10 razones para (des)confiar de las luchas por los derechos humanos*. México: UNAM/Flacso.

Celorio, M. (ed.) (2011). *Internet y dominación, hacia una sociologia de la nueva espacialidad*. México, D. F.: Plaza y Valdés.

Clapham, A. (2006, septiembre). "Obligaciones dimanentes de los derechos humanos para los actores no estatales en situacion de conflcito", *International Review on the Red Cross, 863,* 1-37.

Código Civil Federal (2013).

Cubaencuentro (s/a). "La forma en que pueden ser realizadas las violaciones de los derechos humanos". Recuperado de <http://www.cubaencuentro.com/derechos-humanos/clasificacion-y-caracteristicas/violaciones/la-forma-en-que-pueden-ser-realizadas-las-violaciones-de-los-derechos-humanos>.

Chavez, G. (2015). "Windows 10 quiere llegar a 23 millones de usuarios en México". Recuperado de <http://expansion.mx/tecnologia/2015/07/29/windows-10-quiere-llegar-a-23-millones-de-usuarios-en-mexico>.

El Financiero (video). "Más de 14 mil cámaras en el sistema de Ciudad segura", *Financiero y Bloomberg*.

Gazcón, D. V. (2016). "México, uno de los tres países donde creció la pobreza: Cepal", *Excelsior*, Nacional.

Gobierno de la Ciudad de México (2016). Derechos ARCO. Recuperado de <http://data.finanzas.cdmx.gob.mx/oip/arco/index.html>.

Godoy, E. (2015). "México enredado en la ciberseguridad", *Proceso, Prisma Internacional*.

González, G. (2014). "¿Qué son las cookies de tu navegador y para qué sirven?".

Harvey, D. (2004). "El 'nuevo' imperialismo: acumulación por desposesión". Recuperado de <http://biblioteca.clacso.edu.ar/clacso/se/20130702120830/harvey.pdf>.

Helphone (2011). "La ONU declara a internet como Derecho Humano".

Hoffman, S. (2012). "ONU reconoce los derechos humanos en Internet". *DW* (Derechos Humanos).

INEGI (2015). Número de habitantes. *Cuéntame, población.* Recuperado de <http://cuentame.inegi.org.mx/poblacion/habitantes.aspx?tema=P>.

la.cronica.mx. (2016). "El 73.4% de usuarios en México cuenta con un smartphone", *La Crónica de Hoy* (Negocios).

Ley de Telecomunicaciones y Radiodifusión, 190 C.F.R. (publicada en 2014 y reformada en 2016).

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010).

Madera, F. (2012). "La videovigilancia ya tiene argumentación legal", *Contexto de Durango*.

OHCHR (s/a). *Conceptos clave sobre los DESC. ¿Pueden exponerse algunos ejemplos de violaciones de los derechos económicos, sociales y culturales?* Suiza: Oficina del Alto Comisionado para los Derechos Humanos.

ONU (1948). Declaración Universal de Derechos Humanos. Recuperado de <http://www.un.org/es/documents/udhr/>.

Ortega, J. (2015). "Microsoft admite que espía a usuarios de Windows 10 y esto no puede ser evitado". Recuperado de <http://www.merca20.com/microsoft-admite-que-espia-a-usuarios-de-windows-10-y-esto-no-puede-ser-evitado/>.

R3D.mx (2106). "La SCJN y la #LeyTelecom: lo malo, lo bueno, lo absurdo y lo que sigue".

Secretaría de Gobernación (2016). "El SESNSP presentó la norma técnica que homologará los sistemas de videovigilancia para la seguridad pública del país", *Boletín de prensa*.

UIT-Banco Mundial (2014). *Usuarios de Internet por cada 10, México*. Estados Unidos: Unión Internacional de Telecomunicaciones/Banco Mundial.

Ureste, M. (2016). "Derecho al olvido en internet: ¿un derecho, censura o un redituable negocio en México?" *Animal Político* (Nacional).

[17] Televisiones, computadoras, teléfonos fijos, celulares, aparatos de sonido, video o consolas que han llegado al final de su vida útil. El aumento en la producción y uso de equipo electrónico, aunado a la reducción en el tiempo de vida de dichos productos, eleva cada año el volumen de aparatos obsoletos que son desechados o que quedan almacenados. Las computadoras son un ejemplo representativo. En 1997 una computadora nueva se usaba en promedio seis años; en 2005, dos años. En 1994 se desecharon cerca de 20 millones de computadoras en todo el mundo. Diez años después, fueron más de 100 millones las que dejaron de usarse.