Teknokultura
Revista de Cultura Digital y Movimientos Sociales

#Ricaurte Quijano, P., Nájera, J. y Robles Maloof, J. (2014). Sociedades de control: tecnovigilancia de Estado y resistencia civil en México. *Revista Teknokultura, 11*(2), 259-282.

Recibido: 16-05-2014
Aceptado: 31-07-2014

Link open rewiev:
http://teknokultura.net/index.php/tk/pages/view/opr-224

Sociedades de control: tecnovigilancia de Estado y resistencia civil en México

Societies of Control: State techno-surveillance and Civic Resistance in Mexico

Sociedade de controle: tecno-vigilância de Estado e resistência civil no México

Paola Ricaurte Quijano, Jacobo Nájera y Jesús Robles Maloof
Tecnológico de Monterrey, Campus Ciudad de México - Colectivo Contingente Mx - Colectivo Contingente Mx
pricaurt@itesm.mx – jacobo@metahumano.org
roblesmaloof@gmail.com

Resumen

Este trabajo discute las implicaciones de la vigilancia de Estado a escala global y local a la luz de los planteamientos teóricos sobre las sociedades de control. Sostenemos que la tecno-vigilancia sistemática, permanente y total constituye un hecho innegable que promueve y requiere formas de resistencia civil multivariadas. Para ilustrar nuestro argumento,

realizamos un breve recuento de las acciones emprendidas por la sociedad civil mexicana frente leyes que promueven el uso de la tecnología como instrumento de vigilancia en México, la presencia de *software* espía en los servidores de empresas de telecomunicaciones, y la censura. Por último, presentamos las consecuencias de la tecno-vigilancia en el caso de periodistas, activistas y defensores de derechos humanos. El artículo concluye que los procesos de vigilancia en la sociedades de control se materializan a través de mecanismos socio-técnicos que articulan la esfera pública con la privada, que se realizan con el consentimiento de los sujetos. Sin embargo, esta condición también desencadena formas de resistencia que se manifiestan en la continuidad de lo privado y lo público, lo virtual y lo físico, lo local y lo global.

Palabras Clave

Ciberactivismo, ContingenteMx, control tecnológico, movimientos sociales, neutralidad de la red.

Abstract

The aim of this article is to discuss the global and local implications of State surveillance in the light of the theoretical approach around control societies. We hold that the systematic, continuous and total techno-surveillance is an undeniable fact that promotes and requires multivaried forms of civil resistance. To demonstrate our position, we conducted a brief count of the actions undertaken by the Mexican civil society against the laws that promote the use of technology as a monitoring tool in Mexico, and the presence of spyware in Mexican operators. Finally, we present the consequences of techno-surveillance for journalists, activists and human rights advocates. This article concludes that monitoring practices in control societies are implemented by means of socio-technical mechanisms which articulate the public with the private sphere and are carried out with the civilian consent. However, various forms of civic resistance emerge in the continuity of the private and the public, the virtual and the physical, the local and the global.

Keywords

Cyberactivism, ContingenteMX, technological control, social movements, Net neutrality.

Resumo

Este trabalho discute as implicações da vigilância de Estado em escala global e local sob a luz dos argumentos teóricos a respeito das sociedades de controle. Sustentamos que a tecno-vigilância sistemática, permanente e total constitui um fato inegável que promove e requer formas de resistência civil multivariadas. Para ilustrar nosso argumento, realizamos um breve encontro das ações empreendidas pela sociedade civil mexicana diante das leis que promovem o uso da tecnologia como ferramenta de vigilância, o uso de softwares espiões nos servidores de empresas de telecomunicações e a censura. Por último, apresentamos as conseqüências da tecno-vigilância no caso de jornalistas, ativistas e defensores de direitos humanos. O artigo conclui que os processos de vigilância na sociedade de controle se materializam através de mecanismos sócio-técnicos que articulam a esfera pública com a esfera privada, efetuando-se sem o consentimento dos sujeitos. Entretanto, esta condição também desencadeia formas de resistência que se manifestam na continuidade do privado e do público, do virtual e do físico, do local e do global.

Palavras-chave

Cyber-ativismo, ContingenteMx, controle tecnológico, movimentos sociais, neutralidade da rede.

Sumario

Summary

Sumário

Introducción

Las revelaciones de Edward Snowden respecto al programa de espionaje efectuado por parte de la Agencia Nacional de Seguridad de Estados Unidos constituyen la certeza de la reconfiguración del alcance y naturaleza de la vigilancia masiva, la más ambiciosa conocida en la historia. Es por ello que en este trabajo hemos querido hacer una descripción contextual global y local del papel de la tecno-vigilancia de Estado a partir de los planteamientos teóricos de Deleuze (1992), Hardt y Negri (2000) sobre las sociedades de control. La tecnovigilancia de Estado –sistemática, permanente y total– constituye el fundamento de una sociedad de control global, supranacional (Hardt y Negri, 2000), que bajo una lógica articulada opera a través de entidades de la esfera privada. Más allá de la paranoia orwelliana, la vigilancia masiva constituye un hecho manifiesto que promueve y requiere formas de resistencia civil multivariadas tanto en el ámbito público como privado.

La sociedad de control se sostiene sobre un andamiaje económico, político, jurídico, militar y discursivo que, a través de la infraestructura tecnológica, se inscribe en la intimidad y cotidianidad del sujeto: sus relaciones, su trabajo, sus comunicaciones, su consumo. Frente a este escenario, la sociedad civil debe iniciar acciones de resistencia encaminadas a revertir el uso de la tecnología como instrumento de control tanto en la esfera púbica como privada: desde la capa más profunda, la infraestructura de la red (la propiedad y el control sobre las telecomunicaciones), siguiendo con las conexiones (el tendido de fibra óptica, la provisión de servicios), el desarrollo de *hardware* y *software*, hasta las formas de comunicación (herramientas, servicios) y la cultura digital en general (privacidad, seguridad). Planteamos que las acciones de la sociedad civil deben partir del reconocimiento de los mecanismos de tecno-vigilancia a nivel global y de la necesidad de resistencias que no olviden la continuidad entre lo público y lo privado, lo global y lo local, lo físico y lo virtual. Por tanto, las resistencias deben contemplar la dimensión global de la sociedad de control, los mecanismos de control socio-técnico en sus distintas dimensiones y el papel del sujeto en la reproducción del control a través de la esfera privada.

A manera de ilustración, en este texto realizamos un breve recuento de las acciones emprendidas por la sociedad civil mexicana frente a las diversas iniciativas de leyes que promueven el uso de la tecnología como instrumento de vigilancia masiva en México y ante la presencia de *software* espía en los servidores de empresas de telecomunicaciones identificadas por el *Citizen Lab* (2013, 2014) de la Universidad de Toronto. Además, presentamos

acciones de resistencia de la sociedad civil ante casos emblemáticos de censura digital en el país. Por último, discutimos las implicaciones de los mecanismos de tecno-vigilancia como instrumentos de las sociedades de control y los alcances de la resistencia de la sociedad civil.

Estado del arte

En la coyuntura política global en que vivimos, las evidencias presentadas por Edward Snowden revisten una enorme trascendencia histórica (Der Spiegel, 2013; Macaskill y Dance, 2013; La Quadrature du Net, 2014) y dimensiones inimaginables. A partir de este hecho, es imposible pensar en libertades que no contemplen la dimensión tecnológica. Por ello, si bien es cierto los temas concernientes a la relación entre la tecnología y el poder han sido siempre populares, actualmente el interés general se ha intensificado a partir del descubrimiento de los alcances de la vigilancia masiva, la violación sistemática al derecho a la privacidad de los datos personales y las restricciones a la libertad de expresión en el espacio digital.

En este contexto, los estudios sobre vigilancia se encuentran en un momento de revitalización y resulta frecuente la publicación de libros, números monográficos de revistas, congresos y eventos relativos a este tópico. En la revisión de la literatura especializada encontramos algunas tendencias que orientan la discusión: por una parte, se encuentran los textos que abordan el alcance de las categorías clásicas en los estudios de vigilancia, como el panóptico o el biopoder de Foucault (Lazzarato, 2000; Boyne, 2000; Braga y Vlac, 2004; Lyon, 2006; Caluya, 2010; Mourenza, 2013). Por otra, se analizan casos en los que la censura se realiza o se resiste a través de la tecnología (Verkamp y Gupta, 2013; Winter, 2013, 2014). Un tercer grupo de estudios aborda la naturaleza de las instituciones de vigilancia y espionaje (Fojón y Colom, 2014) y otro documenta los debates que surgen en torno a la democracia y la privacidad (Oliver, 2012; Assange y Romero, 2013).

Este somero vistazo a la reflexión académica sobre la vigilancia y la tecnología pone de manifiesto una inquietud creciente acerca de estos tópicos en el campo científico. Como veremos más adelante, la reacción de las ciudadanías *glocales* también ha colocado en la agenda social, política y mediática esta discusión.

Marco teórico

Michael Foucault (2008) explicó el funcionamiento de la vigilancia y el castigo como la estrategia que utiliza el poder para alcanzar el control y el orden social. Vigilar y castigar se convierten en mecanismos inherentes al funcionamiento de cualquier sistema y el *modus operandi* del poder. Sin embargo, para Foucault, el poder no se realiza en las estructuras o en las instituciones, sino desde dentro, en el cuerpo, a través de la interiorización de las reglas y las prohibiciones por parte de los propios sujetos y de la sujeción tecnológica voluntaria, el poder de la máquina.

La sociedad está constituida por sujetos que habitan las parcelas de sus vidas privadas y sus preocupaciones cotidianas, a la par que ocupan los espacios digitales y físicos de entretenimiento y socialización generados y soportados por la tecnología. La relación del ser humano consigo mismo, con los otros y con el entorno se encuentra mediada por la tecnología, a través de la cual la vida transcurre y se realiza.

En su ensayo *Postdata sobre las sociedades de control* Deleuze (1992), a partir de Foucault, realiza un análisis de la relación entre tipos de máquinas y tipos de sociedad. En un principio, las sociedades de soberanía se encontraban asociadas con maquinarias de mecanismos simples y funcionaban principalmente por una fuerza mecánica; luego, las sociedades disciplinarias, que operaban a través del encierro físico (la casa, la escuela, la fábrica, la cárcel) y máquinas que requerían energías no renovables. Actualmente, dice Deleuze, puesto que nos encontramos en una época de una crisis institucional generalizada ("las instituciones están terminadas"), hemos transitado hacia las sociedades de control:

> Es sencillo buscar correspondencias entre tipos de sociedad y tipos de máquinas, no porque las máquinas sean determinantes, sino porque expresan las formaciones sociales que las han originado y que las utilizan. Las antiguas sociedades de soberanía operaban con máquinas simples, palancas, poleas, relojes; las sociedades disciplinarias posteriores se equiparon con máquinas energéticas, con el riesgo pasivo de la entropía y el riesgo activo del sabotaje; las sociedades de control actúan mediante máquinas de un tercer tipo, máquinas informáticas y ordenadores cuyo riesgo pasivo son las interferencias y cuyo riesgo activo son la piratería y la inoculación de virus. No es solamente una evolución tecnológica, es una profunda mutación del capitalismo.
>
> (Deleuze, 2006, pp.3-4)

Hardt y Negri (2001) plantean que en las sociedades de control el poder se encuentra descentralizado y que la disciplina funciona de manera más profunda, puesto que sus mecanismos abarcan el espacio social y al sujeto mismo:

> Los mecanismos de comando se tornan aún más "democráticos", aún más inmanentes al campo social, distribuidos a través de los cuerpos y las mentes de los ciudadanos. Los comportamientos de inclusión y exclusión social adecuados para gobernar son, por ello, cada vez más interiorizados dentro de los propios sujetos. El poder es ahora ejercido por medio de máquinas que, directamente, organizan las mentes (en sistemas de comunicaciones, redes de información, etc.) y los cuerpos (en sistemas de bienestar, actividades monitoreadas, etc.) hacia un estado de alienación autónoma del sentido de la vida y el deseo de la creatividad. La sociedad de control, por lo tanto, puede ser caracterizada por una intensificación y generalización de los aparatos normalizadores del disciplinamiento, que animan internamente nuestras prácticas comunes y cotidianas, pero, en contraste con la disciplina, este control se extiende muy por fuera de los sitios estructurados de las instituciones sociales, por medio de redes flexibles y fluctuantes.
>
> (Hardt y Negri, 2001, p. 25)

En las sociedades de control, las tecnologías informáticas constituyen el "dispositivo" disciplinario por excelencia, el espacio de realización idóneo para la vigilancia y el castigo. Son formas de control descentralizadas y desterritorializadas (Hardt y Negri, 2000) que se manifiestan fuera de los espacios institucionales estructurados y se instalan en la esfera íntima. El control del sujeto se traduce en una ocupación mediada tecnológicamente de lo íntimo y lo público. Esta ocupación de la vida cotidiana tanto en el espacio físico como en el virtual implica una transgresión por defecto de la privacidad que es asumida como forma natural de la existencia bajo el argumento discursivo de la seguridad: “El biopoder es una forma de poder que regula la vida social desde su interior, siguiéndola, interpretándola, absorbiéndola y rearticulándola” (Hardt y Negri, 2001, p. 25).

La materialización del control sobre el sujeto requiere, además de la interiorización y aceptación voluntaria de las normas disciplinarias, de una infraestructura tecnológica (una computadora, un teléfono móvil, una conexión a internet) e instrumentos (jurídicos, discursivos, políticos, tecnológicos) que suponen la alianza entre el Estado y empresas privadas para poner en marcha los mecanismos de control socio-técnico. A través de los servicios que

ofrecen las empresas de telecomunicaciones se concreta la intervención consentida en la intimidad de la vida del sujeto.

El control socio-técnico: la alianza entre esfera pública y privada

Las filtraciones de Snowden colocaron en la agenda política y mediática a nivel local y mundial la discusión acerca del poder del Estado y los derechos de los ciudadanos. La seguridad es el argumento que sostienen los estados para justificar la vigilancia: un paradigma que se sitúa por encima del derecho a la privacidad. Nos encontramos frente a un falso dilema ético y jurídico que nos demuestra que el derecho a la privacidad, asentado en el artículo 12 de la Declaración Universal de los Derechos Humanos y ratificado por las constituciones de los estados democráticos, enfrenta importantes desafíos en la era digital debido a la disponibilidad de herramientas tecnológicas que permiten recoger información masiva e imperceptiblemente con la colaboración de las empresas privadas. De acuerdo con documentos del servicio británico GCHQ (Government Communication Headquarters), el programa *Dishfire* recopila indiscriminadamente toda la información posible, desde planes de viaje hasta transacciones financieras. Según este reporte, la NSA intercepta millones de registros diariamente. A partir de los avisos de *roaming* se obtienen datos sobre los cruces de frontera y los mensajes en redes sociales permiten obtener los datos geográficos de los usuarios (Ball, 2014; La Jornada, 2014).

Como podemos constatar las técnicas de espionaje y vigilancia que hacen uso de *spyware* son instrumentos invasivos que no se limitan a interferir una comunicación, sino que toman por completo el control de los equipos de cómputo. Es decir, el Estado, a través de empresas de telecomunicaciones, transgrede la esfera privada de los sujetos que han incorporado la tecnología a su vida cotidiana. La recolección de datos personales (*dataveillance*) se ha convertido en la principal forma de vigilancia en la actualidad.

Si bien es claro que todos los estados cuentan con programas de vigilancia, es necesario que cumplan con dos condiciones fundamentales de los sistemas democráticos: la transparencia y la rendición de cuentas. Los estados deben ceñirse a un marco jurídico que defina las condiciones bajo las cuales es posible recolectar información y datos personales de los ciudadanos. En otras palabras: esclarecer quién puede recoger qué tipo de información sobre quién, bajo qué razón legal, con qué objetivos, durante cuánto tiempo y a través de qué medios. Sin embargo, la defensa de un marco jurídico para proteger el derecho a la privacidad se diluye cuando los sujetos aceptan, a cambio de servicios, entregar sus datos personales a

las empresas tecnológicas. Se realiza así, en el sujeto, la consolidación de los mecanismos de vigilancia y control.

La situación de México

En México podemos identificar distintos momentos en la relación entre vigilancia masiva y formas de resistencia civil que buscan revertir los mecanismos de control social. Por una parte se han aprobado leyes que limitan la libertad de expresión y la protección de datos personales (la ley de geolocalización, ley antimarchas, la reforma de las telecomunicaciones). Por otra, se ha detectado *software* de espionaje funcionando en operadores mexicanos (*Finfisher*, *Da Vinci*). Se han lanzado campañas a nivel local y mundial como estrategias de reacción ciudadana (*The Day We Fight Back*, *#StopTheSNA*, *#CensuraMexta*). También se han dado casos específicos de censura, privación de libertad y acoso por acciones de resistencia en el espacio digital (el caso del sitio *1Dmx* o la aprehensión de Héctor Bautista y de Gustavo Maldonado). A continuación revisaremos sintéticamente algunos de estos momentos para ilustrar las tensiones entre los mecanismos de control y las formas de resistencia.

Leyes y políticas

México cuenta con una lamentable trayectoria en la propuesta de iniciativas que involucran la regulación del ciberespacio y el control a través de la tecnología. Se han presentado iniciativas para gravar el uso de Internet (que detonó la campaña *#internetnecesario* en 2009), la firma de acuerdos como ACTA, SOPA, otras propuestas como la Ley Döring, la Ley Duarte, la Ley de Geolocalización, el TPP, la Reforma de las Telecomunicaciones, etc. Algunas de estas iniciativas han sido revertidas por la acción ciudadana, mientras que otras han sido aprobadas por los legisladores.

Con la llamada "guerra contra las drogas" iniciada durante el sexenio de Felipe Calderón, el presupuesto para seguridad creció exponencialmente. Bajo la imposición mediática del discurso sobre la inseguridad en el país, en muy pocos casos las políticas en materia de vigilancia se han cuestionado por parte de la ciudadanía o por los órganos legislativos. No se han fiscalizado las compras de equipo y *software* de los gobiernos con propósitos de seguridad. La interiorización de las formas de control en los sujetos opera no únicamente a través del uso de la tecnología sin una cultura de privacidad y del consenti-

miento a la vigilancia, sino también con el silencio frente a los hechos, las declaraciones, los presupuestos y los actos de violación de derechos por parte del Estado.

La presencia de *software* espía en operadores mexicanos

Tenemos la certeza de la operación de los programas de la Agencia Nacional de Seguridad (NSA) conformados por más de 300 técnicas de ataque, recolección y procesamiento de datos; pero, también hay una serie de empresas dedicadas a la venta de productos y servicios de espionaje que se encargan de distribuirlos a gobiernos, como es el caso de las empresas *Hacking Team, Gamma Group, Trovicor, Blue Coat y Amesys* (RSF, 2014).

FinFisher es el nombre de un equipo de cómputo conformado por *software* y *hardware*. Este *software* espía es capaz de mantener una vigilancia focalizada en el interior de una red informática, desde el monitoreo de llamadas de video y audio, registro de correo electrónico, hasta la posibilidad de controlar la cámara y el micrófono de los equipos de las víctimas (Nájera, 2013). En México fueron encontrados dos de estos equipos tras una investigación del *Citizen Lab* (2013) de la Universidad de Toronto, que consistió en un proceso de *scanning* en las redes. El primero conectado a la red de Uninet de Telmex y el segundo en la de Iusacell. Estos dos equipos de infección a través de *malware*, fueron vendidos a varias secretarías del gobierno mexicano a través de la empresa intermediaria Obses de México.

El *Citizen Lab* (2014) publicó que existen además nodos de distribución de *spyware* de la empresa *Hacking Team* en México. El sistema de vigilancia desarrollado y comercializado por *Hacking Team* se considera una tecnología de seguridad agresiva capaz de instalarse imperceptiblemente:

> El "Remote Control System", comercializado con el nombre de "Da Vinci", es capaz de romper el cifrado y permitir a la policía y servicios encargados de hacer respetar la ley vigilar archivos y correos electrónicos, incluso los que utilizan la tecnología PGP, las conversaciones de Skype y todos los otros protocolos VOIP, así como la mensajería instantánea. Este sistema hace posible la localización de objetivos e identificación de sus contactos, permite activar a distancia cámaras y micrófonos en todo el mundo; pretende que su *software* sea capaz de vigilar simultáneamente centenas de millares de ordenadores en un mismo país; sus caballos de Troya pueden infectar Windows, Mac, Linux, iOS, Android, Symbian y Blackberry.

(RSF, 2014)

Formas de resistencia: las (re)acciones de la sociedad civil mexicana

En el escenario de una sociedad de control global caracterizada por un intenso desarrollo tecnológico, en la que se han generalizado los sistemas de vigilancia masiva por parte del Estado a través de las empresas privadas, sostenemos que es necesario que el sujeto abra espacios de resistencia.

En el caso de México, mientras las organizaciones convencionales han permanecido distantes o subordinadas al control socio-técnico, han surgido pequeños colectivos ciudadanos que han resistido a la vigilancia desde la esfera privada, por ejemplo, a través de redes anónimas que advierten a otros sobre los hechos de violencia de sus localidades. Son conocidas las comunidades digitales *Reynosa Follow*, *Valor por Tamaulipas* o *Valor por Michoacán* por poner algunos ejemplos en los que el anonimato se reivindica como estrategia no solo de resistencia ante las autoridades, sino también frente a los grupos del crimen organizado. Revisaremos algunos casos de resistencia civil frente a las iniciativas de ley, la presencia de *software* de vigilancia masiva y la censura.

La reacción ante las iniciativas de ley

En México se han propuesto y aprobado diversas iniciativas que amplían las capacidades del Estado para el monitoreo de los ciudadanos a través de las empresas proveedoras de servicios de Internet y de telefonía celular (Ley de Geolocalización y Ley de Telecomunicaciones). Durante el periodo previo a la aprobación de estas iniciativas, activistas por los derechos digitales y organizaciones de la sociedad civil desplegaron diversas acciones de resistencia que incluyeron marchas, manifestaciones frente a las sedes del Congreso y el Senado, propuestas técnicas alternativas, cabildeo con los legisladores, cartas de adhesión de personalidades y organizaciones internacionales, artículos en medios y blogs, comunicados, amparos, amicus, campañas digitales, etc. Una cadena humana fue convocada en el Distrito Federal por un grupo de intelectuales, artistas, políticos, sindicalistas, medios comunitarios y activistas en contra de la aprobación de las leyes secundarias en telecomunicaciones.

La solicitud al IFAI por parte del ContingenteMx, Al Consumidor y Propuesta Cívica en el caso *Finfisher*

Las organizaciones civiles ContingenteMx, Al Consumidor y Propuesta Cívica iniciaron una petición ante el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) donde se solicitó investigar la presencia de este *software* bajo el fundamento legal de que las máquinas encontradas por el *Citizen Lab* (2013) permitían el acceso a las comunicaciones de sus víctimas, así como el control de sus computadoras, lo que eventualmente podría constituir una violación a la la Ley de Protección de Datos Personales en México. Las acciones legales tomaron como base cuatro elementos: el primero se refiere a la documentación técnica sobre la operación del equipo *Finfisher*; la segunda fue la investigación realizada por el diario Reforma (2013); la tercera, la argumentación desde la perspectiva de los derechos humanos; y la cuarta, un trabajo de divulgación sobre las implicaciones y peligros para los activistas y periodistas (ContingenteMx, 2013).

Esta petición tuvo como resultado que la empresa intermediaria Obses de México recibiera una sanción por negarse a ser sujeto de la ley. Los proveedores del servicio de Internet (la compañía UNINET de Telmex y Iusacell) afirmaron que bajo su infraestructura no contaban con ese tipo de máquinas, pero no descartaron que sus usuarios, quienes contratan sus servicios, pudieran tener instalado *Finfisher* en algún equipo.

La solicitud realizada al IFAI fue anunciada en conferencia de prensa y retomada ampliamente por diversos medios electrónicos. Los colectivos responsables de la solicitud recibieron numerosas cartas de apoyo por parte de organizaciones internacionales como la *Electronic Frontier Foundation* y personas reconocidas en el ámbito de la defensa de los derechos digitales, como Jacob Appelbaum.

La campaña 13 principios y *The Day We Fight Back*

Los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* (2013) forman parte de un proyecto colaborativo de colectivos sociales preocupados por la privacidad. Estos 13 principios son un instrumento que tiene por objetivo servir de referente para evaluar las leyes relacionadas con la vigilancia masiva y que contempla marcos para aplicar el derecho internacional en el actual entorno digital. Son resultado de un proceso colectivo de discusión de más de un año entre expertos técnicos y defensores de derechos humanos en todo en mundo.

El 14 de febrero de 2014 más de seis mil sitios participaron en una protesta en línea con la finalidad de exigir el fin de la vigilancia masiva. La campaña, bajo el nombre de *The Day We Fight Back*, tuvo un alcance profundo en la red. Entre sus logros, consiguió que más de un millón de personas visitaran su página, 37 millones vieran su *banner*, 550 mil correos se enviaran a representantes, 89 mil llamadas, fuera compartida más de 420 mil veces en Facebook, se publicaran más de 84 mil *tweets* con los *hashtags #StoptheNSA*, *#StopSpying* y *#TheDayWeFightBack*, consiguiendo ser *trending topic* durante la tarde. La campaña promovió también los 13 principios y la recolección de firmas a través de los sitios Change.org y Causes.org. En conjunto consiguieron 301.000 firmas.[1] Organizaciones de la sociedad civil mexicana, entre ellas el *ContingenteMx*, suscribieron los 13 principios y se sumaron a la campaña *The Day We Fight Back*.

El caso *#op1Dmx* y la campaña *#CensuraMexta*

El 1 de diciembre de 2012, día de la toma de posesión de Enrique Peña Nieto como Presidente de México, diversos grupos de la sociedad civil organizaron manifestaciones y actos de repudio frente al Palacio Legislativo de San Lázaro. La convocatoria se difundió en Twitter bajo las etiquetas *#1Dmx* y *#OcupaSanLazaro*. El Estado Mayor Presidencial, apoyado por la Secretaría de Seguridad Pública Federal y la Secretaría de Seguridad Pública del Distrito Federal, desplegó un imponente operativo de seguridad para resguardar el recinto. Se desataron enfrentamientos violentos entre policías y manifestantes, que derivaron en numerosos heridos y detenciones (Contingente Mx, 2014).

Entre las consecuencias de los enfrentamientos están el fallecimiento del profesor Juan Francisco Kuykendall a causa de las lesiones provocadas por la policía; la desaparición de Teodulfo Torres, testigo; la pérdida de un ojo de Uriel Sandoval, uno de los manifestantes; y más de cien detenciones arbitrarias (Contingente Mx, 2014).

Los abusos de autoridad fueron documentados por los periodistas, medios ciudadanos, activistas y por los propios manifestantes. Posteriormente, los registros de la violencia policial fueron recolectados a través de una plataforma digital colaborativa: el sitio 1dmx.org, que sirvió como un espacio de evidencia y denuncia de las arbitrariedades del poder.

[1] La página web de la protesta dedica una estadística pormenorizada de todos los resultados que se obtuvieron. Se encuentra disponible en:
<https://thedaywefightback.org/the-results/>

El 2 de diciembre de 2013, el sitio 1dmx.org fue inhabilitado por *GoDaddy*, la empresa de *hosting* donde estaba alojado. A partir de una solicitud del colectivo *#1Dmx*, la empresa *GoDaddy* reportó que el sitio fue inhabilitado a petición de las autoridades mexicanas, puesto que se encontraba bajo investigación.

El 4 de marzo de 2013 el colectivo *#1Dmx* realizó una rueda de prensa y lanzó la campaña *#CensuraMexta* para denunciar este hecho por parte del Gobierno Federal. Esta denuncia, documentada legal y técnicamente por el colectivo, detonó una reacción por parte de la sociedad civil mexicana, los colectivos de activistas y organizaciones nacionales e internacionales de derechos humanos. *#CensuraMexta* se convirtió en *trending topic* alrededor de las dos de la tarde de ese día. En la Figura 1 se puede apreciar un ejemplo de los contenidos difundidos durante la campaña.

Imagen 1: Denuncia de censura a través de la campaña *#CensuraMexta* en Twitter

Fuente: Twitter.com/CensuraMx

Como consecuencia de la divulgación y la visibilidad mediática del hecho, el sitio fue restablecido sin mayor explicación. Otro ejemplo similar de la incidencia de la presión de la sociedad civil es el caso de las reacciones posteriores a la iniciativa presentada el 24 de

marzo de 2014 por el presidente Enrique Peña Nieto para definir leyes secundarias en materia de telecomunicaciones. Esta iniciativa contemplaba, entre otros puntos, la ampliación de la capacidad de geolocalización por parte de funcionarios del gobierno, la vigilancia masiva, la censura de contenidos y la restricción en el acceso a internet en espacios públicos por razones de seguridad. Las manifestaciones en las calles, el diálogo con legisladores, la presión en medios digitales (*#EPNvsInternet* se convirtió en *trending topic* mundial) entre otras acciones condujeron a posponer la aprobación de la ley al periodo extraordinario de sesiones. A pesar de la presión ciudadana, las leyes secundarias fueron aprobadas con modificaciones menores en julio de 2014.

Las implicaciones de la vigilancia de Estado para periodistas, activistas y defensores

Las investigaciones del *Citizen Lab* (2013) de la Universidad de Toronto demuestran que el *software* de vigilancia ha sido utilizado por los gobiernos para espiar la acción de periodistas, activistas y defensores de varios países.

García (2012) enumera tres tipos de medidas indispensables para que la vigilancia del Estado a través de medios tecnológicos cumpla con los requisitos de legalidad, legitimidad y necesidad:

> 1. La definición clara y precisa en la ley, de los casos y circunstancias en las que dicha medida puede ser adoptada, así como de todas las medidas tendientes a garantizar que la facultad no sea abusada (requisitos de la solicitud, identificación precisa de solicitantes, plazos, procedimiento de manejo, almacenaje y disposición de la información recabada, etcétera).
>
> 2. La autorización y supervisión judicial para la adopción, evaluación permanente o periódica o levantamiento de la medida. Quizá la medida más básica e indispensable.
>
> 3. La existencia de diversas medidas adecuadas y efectivas para prevenir el abuso. Estas medidas pueden consistir en la revisión independiente y periódica del mecanismo y la existencia de recursos adecuados y efectivos.

En el caso de México, hemos sido testigos de numerosos casos en los que se ha vulnerado la privacidad de los datos personales, casos en los que activistas, defensores y periodistas han sido censurados por su actividad u oficio, casos en los que las voces de disenso han intentado ser sofocadas o ciudadanos inocentes injustamente privados de su libertad por

expresiones espontáneas en la red. Entre ellos podemos incluir a Héctor Bautista, Gustavo Maldonado y el uso de *bots* para censurar.

El caso de Héctor Bautista en Chiapas

En septiembre de 2010, ante la censura de algunos de sus artículos en los diarios locales, un grupo de periodistas creó un blog llamado *Informe Chiapas* (infochiapas.com). En septiembre de ese año, el periodista Anthony Flores publicó un análisis sobre la preocupante deuda del gobierno de Juan Sabines, lo que causó molestia en el gobierno. El 3 de noviembre fue detenido Héctor Bautista, webmaster de la página, bajo cargos falsos de pornografía infantil. La movilización nacional de activistas digitales logró que tras 40 días de arraigo Bautista fuera liberado.

El caso del activista Gustavo Maldonado

Uno de los casos que en México ayuda a entender los efectos de la vigilancia y el espionaje, es el del activista digital Gustavo Maldonado, quien fue acusado injustamente por narcomenudeo, y detenido el 8 de agosto de 2013 (Mariscal, 2013). Maldonado fue retenido por 90 días y logró salir bajo caución y llevar su proceso en libertad, gracias a una campaña social desarrollada en Twitter bajo la etiqueta de *#Gumalolibre*, que tuvo como propósito exponer las irregularidades de su caso y evidenciar la conexión existente entre su privación de libertad y el trabajo de denuncia que realizaba contra el gobierno chiapaneco. Él había convocado a movilizaciones por el tema del agua en Tuxtla Gutiérrez, entre otras causas.

Bots para censurar

En años recientes se ha intentado la censura de la opinión por medios indirectos, el *spam* y la programación de *bots* para saturar o para promover ciertos temas en redes digitales como Twitter, una plataforma utilizada como espacio para la expresión de la opinión crítica ciudadana. La ocupación del espacio virtual, principalmente en las plataformas de interacción social, buscan bloquear la opiniones de disenso o la convocatoria a la movilización. Esta estrategia de monitoreo y control del ciberespacio busca crear "realidades" a través del

establecimiento de agendas, la construcción de representaciones e imaginarios sociales a la vez que buscan desalentar e invisibilizar el descontento social.

El estudio de John Paul Verkamp y Miaxi Gupta (2013) de *The School of Informatics and Computing of Indiana University*, recientemente demostró que en China, México, Siria y Rusia se han usado los *bots* masivamente para ahogar las voces disidentes en Twitter, como los *hashtags #MarchaYoSoy132*, *#EPNVeracruzNoTeQuiere* y *#MarchaAntiPeña*. El monitoreo sistemático y el uso de análisis de grandes datos por parte del Estado mediante servicios contratados a compañías privadas, ha permitido colonizar estos espacios e identificar a los actores centrales en los movimientos de protesta.

Discusión

Los mecanismos de control socio-técnico que operan en la sociedad actual se caracterizan por ser sistemáticos, permanentes y totales. El funcionamiento de las herramientas de vigilancia se sostiene en primera instancia en la esfera íntima, micro, por la relación de interdependencia entre tecnología y vida cotidiana; y en la esfera pública, macro, por la participación en un orden mundial de carácter supranacional (Hardt y Negri, 2000) que requiere de la tecnología para operar en todas sus esferas y que además encuentra en el desarrollo tecnológico una forma de realización del poder y del capital.

Las evidencias presentadas sobre los procesos de vigilancia masiva demuestran que en su forma actual se materializan de manera más común a través de los dispositivos personales de los sujetos y que el monitoreo involucra todas sus comunicaciones privadas y desplazamientos; que opera a través de la alianza entre el Estado y la empresa privada; y que se encuentra legitimada a través de un marco jurídico, político y mediático local/global.

La eficacia del sistema de vigilancia radica, en principio, en la participación voluntaria del sujeto en los circuitos de consumo tecnológico, que discursivamente se asume como ineluctable y necesaria. El sujeto consiente tácita y explícitamente su sometimiento a través de sus prácticas cotidianas de comunicación, interacción social, trabajo y entretenimiento. El control del sujeto se traduce en la ocupación, transgresión, resignificación de la esfera privada, lo íntimo, y de la esfera pública, lo abierto.

El régimen panóptico global ha producido sujetos auto-disciplinados, pero a la vez ha dado pie a formas activas de resistencia. A partir de los diversos casos presentados, podemos identificar las siguientes acciones emprendidas por colectivos y personas de la

sociedad civil para enfrentar los procesos de vigilancia sistemática y las limitaciones a la libertad de expresión en México:

1. La documentación del caso específico que permita recabar distintos tipos de evidencia que posteriormente pueden ser utilizados como instrumentos de defensa o de acción.

2. El saber hacer técnico para exponer y hacer visible las capacidades de control en la práctica de cada uno de los servicios y productos de las empresas de telecomunicaciones y los instrumentos de vigilancia.

3. El saber hacer legal, fundamental para la la justificación jurídica y la articulación de la argumentación de la defensa frente a las acciones de vigilancia y censura.

4. La divulgación, para hacer visibles la prácticas tecnológicas de vigilancia, las implicaciones de las políticas, los actores y su operación. El despliegue de campañas de comunicación en espacios digitales, electrónicos y físicos para difundir las demandas ciudadanas y las problemáticas a nivel local y global. La capacitación para desarrollar una cultura digital y de la privacidad de los datos personales.

Conclusiones

En este texto hemos realizado una revisión de los instrumentos tecnológicos y las disposiciones que habilitan la vigilancia en la era digital. También exponemos algunas de las acciones de resistencia desplegadas por parte de la sociedad civil mexicana y tomamos algunos casos emblemáticos de censura en Internet en el país para ilustrar la vigencia y alcance de la vigilancia como herramienta de control socio-técnico.

Una de las tareas que enfrenta la ciudadanía es, por una parte, desde la esfera privada, la comprensión profunda de las implicaciones del control socio-técnico y en esa medida desarrollar una cultura digital y de privacidad de datos personales que vuelva más complejos los procesos de vigilancia. Por otra, en la esfera pública, acotar y delimitar las facultades de las instituciones del Estado a partir de políticas y legislaciones.

Desde la esfera privada, los ciudadanos podemos participar para defender nuestros derechos y los bienes comunes en distintos niveles: habitando internet, tejiendo redes y alianzas globales de resistencia; adoptando buenas prácticas de seguridad; promoviendo el *software* y la cultura libres; investigando y divulgando información relevante sobre el tema; apoyando las iniciativas que promuevan la libertad de internet y el derecho de acceso; votando por aquellos legisladores que se pronuncien abiertamente por defender los derechos de las personas, así como el espectro radioeléctrico e internet. Desde la esfera pública, exigiendo a los gobiernos que construyan una política de Estado desde el principio de la soberanía tec-

nológica, de la concepción del espectro radioeléctrico como un bien público y de internet como procomún. Tener como eje rector a los ciudadanos y sus derechos: garantizar el respeto a la libertad de expresión, el derecho a la información, el derecho de acceso, apropiación y control de las tecnologías de información y comunicación; el derecho a la privacidad de los datos personales y la neutralidad de la red, impedir su control por parte de las corporaciones.

Insistimos en que las formas de resistencia al control socio-técnico requieren de decisiones y acciones deliberadas por parte del sujeto para defender sus derechos. En el escenario de la vigilancia global es indispensable que estas acciones partan de las prácticas y rutinas en su vida privada, que aunadas a la acción colectiva, se traduzcan en conquistas para el espacio público global.

Referencias

Aristegui, C. (2014, 10 de enero). *SCJN valida rastrear celulares; da revés a CNDH* [en línea]. México: Aristegui Noticias. Disponible en <http://aristeguinoticias.com/1001/mexico/scjn-valida-rastrear-celulares-da-reves-a-cndh/> [2014, 18 de mayo]

Assange, J. y P. Romero. (2013). Criptopunks. La libertad y el futuro de internet. *Revista Austral de Ciencias Sociales*, (24), 151-156.

Ball, J. (2014). NSA collects millions of text messages daily in 'untargeted' global sweep. *The Guardian* [en línea]. Disponible en <http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-swee>

Borde Jurídico (2014). *#LeyGeolocalización en SCJN. Un recuento*, [en línea]. Disponible en <https://www.facebook.com/photo.php?fbid=709097059130984&set=a.681822371858453.1073741826.633234383383919&type=1&theater>

Boyne, R. (2000). Post-panopticism. *Economy and Society*, Volume 29, Issue 2, 285-307.

Braga, S. y Vlac, V. (2004). Os usos políticos da tecnologia, o biopoder e a sociedade de controle: considerações preliminares. Scripta Nova. *Revista electrónica de geografía y ciencias sociales*, 8(170). Disponible en <http://www.ub.es/geocrit/sn/sn-170-42.htm>

Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. *Social Identities*, Vol. 16, No. 5, 621-633.

Citizen Lab (2013, 13 de marzo). *You Only Click Twice: FinFisher's Global Proliferation* [en línea]. Universtiy of Toronto. Disponible en <https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/> [2014, 18 de mayo]

Citizen Lab (2014, 17 de febrero). *Mapping Hacking Team's "Untraceable" Spyware* [en línea]. University of Toronto. Disponible en <https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/>

Comisión Nacional de Derechos Humanos (2012). *Demanda de acción de inconstitucionalidad, promovida por la Comisión Nacional de los Derechos Humanos* [en línea]. Disponible en <http://www.cndh.org.mx/sites/all/fuentes/documentos/CorteInteramericana/DEMANDA%2032-2012.pdf>

ContingenteMx (2013, 7 de octubre). *Comunicado de Prensa sobre los avances en las investigaciones sobre FinFisher en México*. Blog [en línea]. Disponible en <http://contingentemx.net/2013/10/07/comunicado-de-prensa-sobre-los-avances-en-las-investigaciones-sobre-finfisher-en-mexico/>

ContingenteMx (2014, 3 de marzo). *Spyware de la empresa Hacking Team opera bajo redes mexicanas*. Blog [en línea]. Disponible en <http://contingentemx.wordpress.com/2014/03/03/spyware-de-la-empresa-hacking-team-opera-bajo-redes-mexicanas/?preview=true&preview_id=480&preview_nonce=29342106a2&post_format=standard>

Deleuze, G. (1992). Postscript on the Societies of Control. *October*, Vol. 59, pp. 3-7.

Deleuze, G. (2006). Postdata sobre las sociedades de control. *Polis. Revista Latinoamericana*, No. 13. Disponible en <http://polis.revues.org/5509>

Fojón, E., y Colom, G. (2014). La NSA en la era del ciberespionaje masivo. *Política Exterior*, 28(157), 34-39.

Foucault, M. (1995). El sujeto y el poder. En Terán, O. Michel Foucault. *Discurso, poder y subjetividad*. Buenos Aires: El Cielo por Asalto.

Foucault, M. (2008). *Vigilar y castigar. Nacimiento de la prisión*. México: Siglo XXI.

García, L. F. (2012, 21 de febrero). *La (in)constitucionalidad de la #LeyGeolocalización. Human Rights Geek*. Blog [en línea]. Disponible en <http://humanrightsgeek.blogspot.mx/2012/02/la-inconstitucionalidad-de-la.html>

García, L.F. (2014, 14 de enero). *La Corte y sus (malos) argumentos a favor de la geolocalización de celulares sin controles. El Juego de la Suprema Corte*. Blog [en línea]. Disponible en <http://eljuegodelacorte.nexos.com.mx/?p=3507#sthash.tTsAg2Eu.dpuf>

Interactive Graphics: The NSA's Spy Catalog. (2013, 30 de diciembre), [en línea]. Alemania: Spiegel Online International. *Der Spiegel*. Disponible en <http://www.spiegel.de/international/world/a-941262.html>

Hardt, M. & Negri, A. (2000). *Empire*. Cambridge, MA: Harvard University Press.

Hardt, M. y Negri, A. (2001). *Imperio*. Bogotá: Ediciones Desde Abajo.

La Jornada. (2014, 17 de enero). La NSA obtiene 200 millones de mensajes de texto al día. Wikileaks en *La Jornada* [en línea]. Disponible en <http://wikileaks.jornada.com.mx/notas/la-nsa-obtiene-200-millones-de-mensajes-de-texto-al-dia#sthash.PGpS9mYB.C1N52lT9.dpuf>

La Quadrature du Net. (2013). *Things the NSA doesn't want you to know And why you should know about it* [en línea]. Disponible en <https://nsa-observer.laquadrature.net/>

Lazzarato, M. (2000). Du biopouvoir à la biopolitique. *Multitudes*, (1), 45-57.

Lyon, D. (Ed.). (2006). *Theorising surveillance: The panopticon and beyond*. Uffculme, Devon: Willan Publishing.

Macaskill, E. y Dance, G. (2013, 1 de noviembre). NSA Files Decoded. What the revelations mean to you. *The Guardian* [en línea]. Disponible en <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>

Mariscal, A. (2013). Gumalo, activista de las redes sociales, enfrentará juicio en libertad. *Chiapas Paralelo* [en línea]. Disponible en <http://www.chiapasparalelo.com/noticias/chiapas/2013/11/gumalo-activista-de-las-redes-sociales-enfrentara-juicio-en-libertad/>

Mourenza, D. (2013). Dreams of a Better Nature: Walter Benjamin on the Creation of a Collective Techno-Body. Revista *Teknokultura*, 10(3), 693-718.

Nájera, J. (2013). El espionaje digital como servicio. *El Toque. Blog* [en línea]. Disponible en <https://eltoque.com/texto/el-espionaje-digital-como-servicio>

Oliver, M. C. (2012). El caso WikiLeaks como piedra de toque de la democracia deliberativa de Jürgen Habermas. *Dilemata*, (8), 123-151.

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (2013, julio 10) en *Necessary and Proportionate*. Disponible en <https://en.necessaryandproportionate.org/text/2013/07/10>

Reforma (2013, 7 de julio). *Paga SSP 673 mdp a firma de 'spyware' en Reforma* [En línea]. Disponible en
<http://bit.ly/1k6olRQ>
<http://busquedas.gruporeforma.com/reforma/BusquedasComs.aspx#ixzz38vD1XE6E>

RSF. (2014, 12 de marzo). *Empresas enemigas de Internet en Enemigos de Internet*. Reporte 2013 [en línea]. Disponible en
<http://surveillance.rsf.org/es/category/empresas-enemigas-de-internet/>

Verkamp, J. P., y Gupta, M. (2013). *Five incidents, one theme: Twitter spam as a weapon to drown voices of protest*. [en línea]. Workshop on Free and Open Communications on the Internet. 3rd USENIX Washington, D.C. Disponible en
<http://0b4af6cdc2f0c5998459-c0245c5c937c5dedcca3f1764ecc9b2f.r43.cf2.rackcdn.com/12385-foci13-verkamp.pdf>

Winter, P. (2013, 13 de agosto). *Towards a Censorship Analyser for Tor. [en línea]*. *Workshop on Free and Open Communications on the Internet. 3rd USENIX*. Washington, D. C. Disponible en
<https://www.usenix.org/conference/foci13/workshop-program/presentation/winter>

Winter, P. (2014, mayo). *Enhancing Censorship Resistance in the Tor Anonymity Network*. Trabajo de grado, Ciencias de la Computación. Karlstad University, Karlstad. Disponible en
<http://www.diva-portal.org/smash/get/diva2:680558/FULLTEXT01.pdf>