#RICAURTE, P. (2015). Desafíos de la acción colectiva en la era post-Snowden: lecturas desde América Latina, *Vol. 12*(3), 429-447.

Recibido: 27-11-2015
Aceptado: 05-12-2015

Open peer review
http://revistas.ucm.es/index.php/TEKN/pages/view/opr-51340

Desafíos de la acción colectiva en la era post-Snowden: lecturas desde América Latina

Challenges to collective action in the post-Snowden era: visions from Latin Americay

Paola Ricaurte
Instituto Tecnológico de Monterrey
pricaurt@itesm.mx

RESUMEN

Este artículo busca por una parte, introducir las contribuciones que forman parte del monográfico "Los desafíos de la acción colectiva en la era post-Snowden: lecturas desde América Latina" y por otra, hacer un llamado a continuar el debate en nuestro contexto sociocultural. La tecnovigilancia se encuentra en el centro de un sistema regulatorio de las relaciones, interacciones y conductas del sujeto en la sociedad contemporánea. Partimos de la premisa de que existe una articulación de fuerzas entre las instituciones del Estado, las empresas proveedoras de servicios de telecomunicaciones, la industria de los datos personales y la industria mediática que construyen dispositivos tecnológicos, financieros, narrativos, analíticos y jurídicos para la legitimación de la vigilancia. Los resultados se plasman en leyes, la construcción de imaginarios, eventos, discursos, artefactos, formas de interacción y

espacios para vigilar. La vigilancia selectiva y masiva ocupan las esferas pública y privada, ponen en discusión la comprensión sobre la intimidad, la libertad de expresión, la seguridad, las relaciones sociales, el ejercicio de la ciudadanía. Esta coyuntura demanda una reflexión sobre los ejes de la resistencia y las posibilidades de la acción colectiva, su análisis en el marco de las sociedades de control y la identificación de los mecanismos que entran en juego para su ejecución.

Palabras Clave

Dispositivos; sociedades de control; tecnovigilancia; vigilancia masiva; vigilancia selectiva.

Abstract

This article aims to introduce the contributions to the monograph "The challenges of collective action in the post-Snowden era: readings from Latin America" and is intended to promote further discussion in our social and cultural context. Techno-surveillance is located in the center of a regulatory system of relationships, interactions, and behaviours in contemporary societies. We argue that state institutions, Internet Service Providers, industries of personal data and surveillance, and the media are acting as articulated forces. Technological, financial, narrative, and legal devices are created to legitimate surveillance. The implications are reflected in the production of laws, artifacts, events, discourses, imaginaries, cultural practices, bodies and places for surveillance. Surveillance questions our understanding of privacy, freedom of expression, security, social relations, and the exercise of citizenship. Targeted and mass surveillance shape both public and private spheres. This fact demands a reflection on the possibilities of collective action and resistance. Analytical frameworks are needed to identify the mechanisms and implications of the surveillance society.

Keywords

Devices; control societies; technosurveillance; mass surveillance; targeted surveillance.

Sumario

Introducción
Ensamblaje teórico
Vigilancia: un fenómeno multidimensional
América Latina: la emergencia del Estado vigilante
La era era post-Snowden: llamado a la acción
Cierre
Referencias

Summary

Introduction
Theoretical framework
Surveillance: a multidimensional phenomenon
Latin America: the rise of the surveillance State
The Post-Snowden era: call to action
Closing
References

Introducción

A partir de las revelaciones de Edward Snowden constatamos que en la actualidad vivimos en sociedades de control (Deleuze, 2006) en las que las infraestructuras tecnológicas son utilizadas como dispositivos disciplinarios de la subjetividad (Hardt y Negri, 2001). Las miradas, las relaciones, los afectos, las sensaciones se ajustan a los esquemas modalizantes del capitalismo cognitivo (Moulier-Boutang, 2011). A diferencia de otras épocas, el alcance, la sofisticación y los mecanismos de sujeción se han ampliado, se encuentran descentralizados, abarcan actores de la esfera pública y privada, y se ejecutan a partir de la participación activa de los propios sujetos de la vigilancia.

Los sistemas de tecnovigilancia se inscriben en el corazón de las sociedades de control (Deleuze, 2006) como uno de los dispositivos (Deleuze, 1992) materiales, sociales, narrativos, financieros que se articulan para garantizar la eficiencia de su funcionamiento. En la diversidad y complejidad de los contextos latinoamericanos, las construcciones discursivas provenientes de las instituciones del Estado toman la inseguridad, la violencia o las tensiones políticas como el argumento para la naturalización del Estado de excepción (Agamben, 2005), reforzar la inversión en infraestructura de vigilancia, la promoción de mecanismos jurídicos que avalen su despliegue masivo y la normalización social de la cultura de la vigilancia.

Las evidencias sobre las millonarias inversiones en tecnología de vigilancia en América Latina, así como la propuesta de leyes que facultan la vigilancia en países como México, Perú, Paraguay, Ecuador, por nombrar algunos casos, han sido documentadas por organizaciones de la sociedad civil en distintos países latinoamericanos (Rodríguez, 2015), por informes de centros de investigación especializados (Citizen Lab, 2014, 2015) y más recientemente por filtraciones de Wikileaks (2015). Los documentos filtrados han demostrado que los países de América Latina, en particular México (ContingenteMx, 2014) y Chile, constituyen sólidos clientes de la empresa Hacking Team, declarada por la organización Reporteros sin Fronteras (2014) como uno de los enemigos de internet.

El nulo resultado en la mejora de las condiciones de seguridad o en el control del crimen, la recurrente persecución de activistas, defensores y periodistas, la privación del derecho a la libertad de expresión a través de dispositivos tecnológicos, la tortura y el asesinato de luchadores sociales demuestran que la enorme capacidad de vigilancia que poseen algunos gobiernos latinoamericanos no se utiliza con fines de seguridad y combate a la delincuencia,

sino primordialmente con fines políticos. Los ciudadanos latinoamericanos nos encontramos expuestos principalmente a la tecnovigilancia ejercida por parte de la Agencia Nacional de Seguridad (NSA, por sus siglas en inglés) y la Administración para el Control de Drogas (DEA, por sus siglas en inglés) de Estados Unidos, y a nivel local por parte de los estados nacionales y sus diversas dependencias. En consecuencia, estamos sujetos a la violación sistemática de nuestros derechos a través de la privación de la libertad física y la libertad de expresión.

Esta coyuntura es fundamental para replantear cualquier estrategia de acción colectiva encaminada a promover el cambio social. Sostenemos que la discusión debe situarse en un plano crítico y multidimensional que evalúe las complejas articulaciones entre la economía, las infraestructuras tecnológicas, las infraestructuras mediáticas, la dimensión político-jurídica y los procesos de acción social tanto en el plano local como global. Planteamos que es necesario ponderar los objetivos, alcances, estrategias, prácticas, principios de organización, procesos de comunicación y acciones de resistencia de los actores de la sociedad civil latinoamericana frente al fortalecimiento de los estados vigilantes.

Es por esta razón que quisimos plantear algunos posibles ejes de discusión que pusieran el acento en las relaciones entre acción colectiva y vigilancia, derechos humanos, los contextos políticos diversos, los marcos jurídicos, la economía de la información y la industria de los datos personales, las capacidades de vigilancia de los estados y su relación con el sistema global de vigilancia y la industria, las formas de resistencia de los sujetos vigilados o su seducción por parte de de narrativas para legitimar la vigilancia.

En este artículo haremos una introduccion a la discusión sobre la vigilancia y sus dimensiones; de manera que sirve como presentacion de las contribuciones que forman parte del monográfico “Los desafíos de la acción colectiva en la era post-Snowden: lecturas desde América Latina”. Este ejercicio colectivo multinacional es un llamado a continuar el debate a partir de nuestro contexto sociocultural.

Ensamblaje teórico

El debate acerca de la vigilancia es antiguo, amplio y cada vez más complejo. La transformación de los mecanismos y alcances de la vigilancia a partir del desarrollo de tecnologías con mayores capacidades: más intrusivas, imperceptibles y sofisticadas que operan en los ámbitos más íntimos de la vida cotidiana través de todas sus facetas (rastreo, extracción, registro y al-

macenamiento de datos), le ha otorgado a la vigilancia una nueva dimensión que se refleja en el debate académico y también social.

La creciente literatura que alimenta el campo de los estudios sobre vigilancia se orienta a estudiar la vigilancia a partir de diversas tradiciones teóricas y metodológicas que muestran la complejidad del fenómeno y la necesidad de miradas cada vez más transdisciplinarias. En lo que respecta a los fundamentos teóricos, las principales aportaciones contemporáneas abordan la vigilancia a partir de la herencia intelectual de Foucault, Baudrillard, Deleuze, Bauman, Giddens, Latour, Agamben, Hardt y Negri, por mencionar solamente a los más citados y discutidos. Podríamos decir que a partir del desarrollo y el alcance masivo de las tecnologías de la vigilancia, nos encontramos en una nueva época que busca discutir las categorías tradicionales: el panóptico y el biopoder (Foucault, 2006, 2008), el sinóptico (Mathieson, 1997), el post-panóptico (Boyne, 2000), las sociedades de control (Deleuze, 2006; Hardt y Negri, 2001), el ensamblaje de la vigilancia (Deleuze y Guattari, 2004; Haggerty y Ericson, 2000) o la vigilancia líquida (Bauman y Lyon, 2013); y ponerlas a prueba o en tela de juicio a partir de nuestro actual contexto tecnológico y social. El debate incorpora nuevas discusiones acerca del cuerpo como información o el sujeto como dato, la internalización de la mirada (Simon, 2002) y se mantiene vigente la tensión entre la vigilancia como control (Giddens, 1987), simulación (Bogard, 1996), seducción (Bauman, 1988), placer o resistencia (Critical Art Ensemble, 2001).

La tecnovigilancia en la era contemporánea puede abarcar desde la vigilancia de los consumidores (consumer surveillance) hasta la vigilancia como parte de los sistemas burocráticos institucionales, financieros u organizacionales. Estos tipos de vigilancia dan paso a un nuevo ámbito que reduce el sujeto a su representación en datos y transforma su circulación en flujos de datos (Lyon, 2006). Este nuevo dominio de la vigilancia o *dataveillance*, se define como el monitoreo sistemático de las acciones o comunicaciones de las personas a través de tecnologías de la información (Clarke, 1988) que involucra también su registro y posterior análisis con fines específicos. El tipo de vigilancia que nos ocupa aquí es la vigilancia promovida y operada por el gobierno y que se apoya en la alianza con las empresas de telecomunicaciones y las boyantes industrias de la seguridad y de los datos personales. Bauman y Lyon (2013) sostienen que nos encontramos en una fase de vigilancia líquida correspondiente a un Estado líquido en constante dinamismo, con fronteras difusas, en el que los sujetos en movimiento se encuentran sistemáticamente monitoreados.

Asumimos la perspectiva teórica que plantea que la vigilancia constituye parte de un ensamblaje (Deleuze y Guattari, 2004) de distintos dispositivos (Deleuze, 1992) técnicos, jurídicos, económicos, discursivos en los que el ejercicio del poder se realiza principalmente a través de la cotidianidad y la vida íntima del sujeto-dato. Sostenemos que la tecnovigilancia de Estado sistemática, masiva y sin contrapesos constituye el fundamento de una sociedad de control global, supranacional (Hardt y Negri, 2001), que bajo un discurso articulado y coherente entre los distintos actores (gobierno, empresas, medios, industria de la seguridad) opera a través de entidades de la esfera privada. (Ricaurte *et al*. 2014)

La vigilancia: un fenómeno multidimensional

Si bien las revelaciones de Edward Snowden contribuyeron a colocar la vigilancia masiva en la agenda mediática, no es el único escenario sobre el que debe centrarse la discusión. La vigilancia, como proceso multidimensional y complejo, involucra actores, narrativas, artefactos, condiciones y procesos en relaciones de profunda interdependencia. A continuación proponemos algunos ejes y cuestionamientos que pueden contribuir a la reflexión crítica sobre este tema y a orientar la acción colectiva en las sociedades vigilantes.

La perspectiva de los derechos humanos

Desde la perspectiva de la persona, la vigilancia debe situarse en un marco de respeto irrestricto a los derechos humanos. De acuerdo con Frank La Rue (2013), ex Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión para las Naciones Unidas:

> La vigilancia de las comunicaciones debe considerarse un acto sumamente perturbador que podría suponer una injerencia en los derechos a la libertad de expresión y la intimidad, y que atenta contra los fundamentos de una sociedad democrática. La legislación debe estipular que la vigilancia de las comunicaciones por el Estado solo se realice en las situaciones más excepcionales y únicamente con la supervisión de una autoridad judicial independiente. La legislación debe incluir salvaguardias relativas a la naturaleza, el alcance y la duración de las posibles medidas, los motivos que se requieren para disponerlas, las autoridades com-

> petentes para autorizarlas y supervisarlas y el tipo de reparaciones previstas en la legislación nacional.
>
> (La Rue, 2013)

El derecho a la privacidad[1] se diluye en este nuevo marco de vigilancia masiva y se relega como un estatuto secundario de la persona, disociando su vinculación con el derecho a la libertad de expresión y por tanto el derecho a la libertad en general.

El marco jurídico

Existe una tendencia global a reforzar las leyes que posibilitan la vigilancia masiva, su alcance y su duración. De manera paralela, se promueven leyes que castigan los mecanismos y las prácticas de protección de la privacidad por parte de los usuarios. La criminalización del anonimato, el recrudecimiento de las leyes con relación al cifrado y la responsabilidad de los intermediarios son prácticas globalmente extendidas. En el actual contexto político mundial, especialmente en el contexto de las tensiones que se han generado frente al estado islámico, se han desencadenado una serie de reacciones que tienden a justificar la vigilancia irrestricta a partir de un estado de excepción en el continente europeo que tienen consecuencias en todo el mundo.

La construcción de narrativas

Por una parte, la vigilancia se encuentra sustentada por las leyes como un instrumento fundamental para mantener la seguridad de los estados, que extienden la vigilancia como práctica sistémica. Sin embargo, para poder legitimarla requieren de la construcción de discursos que

[1] El Derecho a la intimidad o la privacidad de las personas es un derecho humano.El Artículo 12 de la Declaración Universal de los Derechos Humanos, adoptada por la Asamblea General de las Naciones Unidas, establece que el derecho a la vida privada es un derecho humano, y que: "Nadie será objeto de injerencias arbitrarias en su vida privada, ni su familia, ni cualquier entidad, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

En la Convención Americana de Derechos Humanos el artículo 11 declara que: 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

se instalan en el imaginario social y contribuyen a que los sujetos la incorporen como un elemento necesario para la realización de la vida cotidiana. Resulta indispensable el análisis de esas narrativas sobre la privacidad y la seguridad que se construyen en la alianza del aparato político con el mediático y con la injerencia directa de la propia industria de la vigilancia.

La dimensión económica

En la llamada sociedad de la información y del conocimiento los datos personales se convierten en un nuevo capital. La extracción de datos personales (data mining) a nivel masivo (big data) por parte de las empresas de telecomunicaciones se suma a los datos generados por parte de la industrias de seguridad y vigilancia a través de dispositivos que ocupan el espacio público (videocámaras, drones) y privado (wearables, dispositivos móviles). Los distintos sistemas de seguridad se publican y se comercializan a través de eventos (ContingenteMx, 2015) y acuerdos realizados directamente entre las empresas de vigilancia y los estados.

La dimensión tecnológica

Los dispositivos tecnológicos constituyen el mecanismo material a través del cual se realiza la vigilancia. Junto al software espía hay todo un abanico de piezas de hardware que participan en el proceso: videocámaras, drones, teléfonos celulares, computadoras, aplicaciones, plataformas de interacción social, videojuegos, wearables, así como todos los artefactos del universo del internet (historiales de navegación, cookies, puertas traseras) y del internet de las cosas. A todos estos elementos se le suman a otro conjunto de dispositivos no materiales (el sistema financiero, los sistemas de análisis de big data, las leyes, los medios, etc.) que también son fundamentales para la operación del sistema.

Frente a todos estos dispositivos existen diversas expresiones de acción colectiva, disidente o resistente, protagonizadas por actores ciudadanos que desarrollan estrategias para contestar la vigilancia y llaman a la desobediencia civil electrónica (Critical Art Ensemble, 2001), la soberanía tecnológica (Rhizomatica, 2015), el cifrado (Assange, Müller-Magnug, Appelbaum, 2012) o el hackeo de infraestructuras que trastoquen o subviertan los mecanismos vigilantes. El ejercicio del anonimato en red, la búsqueda de soluciones técnicas para alcanzar la soberanía tecnológica y la seguridad del sistema de cifrado, el abandono de las plataformas y el

rechazo de las corporaciones que se lucran con los datos, son algunas de las acciones orientadas a relacionarse críticamente con las estructuras sociotécnicas.

La dimensión política

En los estados latinoamericanos con gobiernos de diferentes espectros políticos y niveles de democracia, en años recientes se han propuesto leyes que facultan la vigilancia sin contrapesos y que promueven la inversión en presupuesto para la compra de hardware y software espía bajo el argumento de la seguridad y la defensa nacional. Esta situación plantea algunas interrogantes: ¿Qué pasa cuando la vigilancia se encuentra enmarcada en un sistema de corrupción? ¿Qué implica vigilar como un arma política?¿Qué relación existe entre los intereses políticos y la industria de la vigilancia?

Los actores ciudadanos deben demandar que la vigilancia ejercida por los gobiernes se ajuste estrictamente a los 13 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (2013) y que no sea utilizada como una herramienta de control político. Además, deben existir contrapesos jurídicos a la vigilancia y el establecimiento de mecanismos efectivos de transparencia y rendición de cuentas, exigir a los estados que se hagan públicas las inversiones, los procesos de licitación y compra de software y hardware destinado a la vigilancia.

El cuerpo vigilado

¿Qué ocurre cuando el sujeto/cuerpo se convierte en el objetivo y principal fuente de información? ¿Cómo se produce la internalización de la mirada en el sujeto vigilado? ¿Qué dimensión ocupa el género? ¿Cómo se establecen las tensiones entre el observado y el observador? ¿Quién observa? El sujeto-dato, el cuerpo-dato son el lugar de ejecución de la vigilancia. La sofisticación de los sistemas biométricos, los equipos de reconocimiento facial, los dispositivos que se desarrollan para tal efecto hacen que la identificación del sujeto, a través de su ADN, sus huellas digitales, su iris, generen un banco de datos que un sujeto difícilmente puede evadir para defender su privacidad.

Los actores

A medida que se adoptan más leyes para promover la vigilancia y se desarrollan tecnologías cada vez más complejas, los sujetos de vigilancia se encuentran inmersos en procesos que involucran actores públicos y privados, individuales y colectivos, a nivel local y global: ¿Quiénes son los actores de la vigilancia? ¿Cómo se establecen esos procesos y esas relaciones en torno a la vigilancia cuando hablamos de gobiernos nacionales e internacionales, corporaciones, instituciones, crimen organizado y sociedad civil? Descubrir el entramado de relaciones de poder, financieras y políticas, constituye un punto de partida fundamental para la comprensión de la conformación y desarrollo de los sistemas de vigilancia.

América Latina: la emergencia del Estado vigilante

Aunque históricamente ha existido conciencia de los sistemas de vigilancia, las declaraciones de Snowden marcaron un antes y un después al proporcionar del alcance extraterritorial y los mecanismos de la vigilancia global. La actividad de la Agencia Nacional de Seguridad y la Administración para el Control de Drogas en la región, sumada a la compra de equipo por parte de los gobiernos nacionales han generado innumerables reacciones de la sociedad civil organizada latinoamericana que ha insistido en la necesidad de exigir transparencia, rendición de cuentas sobre el uso de este tipo de tecnologías y respeto de los derechos humanos. (Rodríguez, 2015)

Durante el mes de julio de 2015 se filtraron una serie de documentos que contenían información sobre la actividad comercial de la empresa Hacking Team (hackingteam.it). Los documentos incluían contratos, contactos, propuestas de venta de software y capacitación a países de América Latina (Wikileaks, 2015). El tipo de software comercializado por la empresa es sumamente intrusivo (HackingTema, s/f) y posee la capacidad de extraer datos personales sensibles infectando sus propios dispositivos tecnológicos. Además, puede tomar control de los equipos (activación de cámara, audio y video) sin que el usuario o los programas antivirus lo identifiquen. México, Ecuador, Colombia, Chile, Honduras y Panamá se encontraban en la lista de clientes de Hacking Team, con inversiones millonarias y con la participación de diversas dependencias de los estados, no necesariamente relacionadas con actividades de inteligencia. En México, destacan como colaboradores de la operación: Petró-

leos Mexicanos, la Secretaría de Marina (SEMAR), el gobierno de los estados de Puebla, Durango, Tamaulipas, Campeche, Yucatán, la Procuraduría General de Justicia, la Policía Federal; en Ecuador, la Secretaría de Inteligencia de Ecuador (SENAIN); en Colombia, la Dirección de Inteligencia Policial de Colombia (DIPOL); en Chile, la Policía de Investigaciones de Chile (PDI).

El fortalecimiento del Estado vigilante en América Latina ha estado acompañado del surgimiento de colectivos y organizaciones cuya agenda se diversifica entre la demanda por mayor transparencia y rendición de cuentas, la seguridad digital, la soberanía tecnológica, el internet libre y el apego a derechos a través de la suscripción a los 13 Principios, que constituyen un marco internacional para guiar los procedimientos y alcance de la vigilancia de las telecomunicaciones. Algunos de estos colectivos para el caso de México son el Rancho Electrónico, ContingenteMx, Enjambre Digital, Red de Defensa de Derechos Digitales, Artículo 19, Primero de Mayo; en Colombia, la fundación Karisma y RedPato2; en Chile, la organización Derechos Digitales; en Ecuador, Fundamedios y Usuarios Digitales; en Argentina, Vía Libre; en Perú, Hiperderecho;entre muchos otros. Además, organizaciones internacionales apoyan las iniciativas orientadas a la defensa de derechos en el entorno digital en América Latina, como la Electronic Frontier Foundation, Access, The Web Foundation, Global Voices, Mozilla Foundation, Wikimedia Foundation, Free Software Foundation, Tactical Tech, Ford Foundation, Coding Rights, Article 19 (global). Actores internacionales relevantes en el debate sobre internet y los derechos humanos también han participado para impulsar las acciones frente a la vigilancia en América Latina, entre los que destacan Julian Assange, Edward Snowden, Jacob Appelbaum, Jérémie Zimmerman y Richard Stallman.

La era post-Snowden: llamado a la acción

Los textos que componen este monográfico abordan desde aproximaciones diversas la problemática de la vigilancia. Dan cuenta de las acciones, relaciones, discusiones y tensiones en torno a la vigilancia en el contexto latinoamericano. La heterogeneidad de las perspectivas permite enriquecer y ampliar el debate que en ocasiones suele enmarcarse en la perspectiva de derechos humanos.

Para incorporar la reflexión sobre la mirada y el poder desde una perspectiva sociotécnica, el texto de Pablo de Soto Suárez "#DroneHackademy: contravisualidad aérea y ciencia ciudadana para el uso de UAV como tecnología social" presenta un caso en el que desde la ciencia

ciudadana, como experiencia de aprendizaje en comunidad, se busca subvertir el régimen de visualidad contemporáneo. Los Vehículos Aéreos No Tripulados (UAV), drones, son reconvertidos simbólicamente en artefactos a través de los cuales es posible materializar el derecho a la mirada. La mirada como ejercicio de poder y el dron como dispositivo, son capaces de subvertir la visión panóptica de la sociedad vigilante, que se apropia también del espacio aéreo.

Para continuar, Alejandra López Gabrielidis en "Régimen de visibilidad y vigilancia en la era de la identidad digital" amplía la discusión a través del análisis de los mecanismos de subordinación del sujeto a la hipervisibilidad. En un estudio de la obra audiovisual de Hito Steyerl contrasta los anteriores dispositivos de vigilancia con los actuales. Destaca el papel del sujeto como agente activo de la vigilancia, a través de sus prácticas cotidianas en la red, que lo hacen partícipe y co-responsable del régimen de vigilancia.

En un abordaje desde la dimensión política, Iria Puyosa en "Control político de internet en el contexto de un régimen híbrido" habla del caso de Venezuela durante 2007 a 2015. Analiza las políticas de control del Estado venezolano sobre Internet y la red participativa. A partir de este ejercicio, busca demostrar la vinculación entre las políticas públicas y la práctica de control político.

En el texto "Estructura institucional e intoxicación informativa: polarización política y derechos digitales en la República de Ecuador", Efrén Guerrero aborda las limitaciones de la acción colectiva cuando existe un desequilibrio de fuerzas entre los actores políticos y sociales. A partir del caso ecuatoriano, muestra los obstáculos que presenta la participación en redes sociodigitales donde prevalece la polarización y la dicotomización, un espacio de disputa y control.

Bernardo Gutiérrez en "Criptopunks y América Latina: de la soberanía tecnológica a la era de las filtraciones" aborda la incidencia de los hackers globales en las dinámicas y políticas de los países latinoamericanos a través de un análisis del caso de Brasil y la aprobación del Marco Civil de Internet. La legislación, pionera y de vanguardia con respecto a la defensa de un internet libre, fue aprobada en 2014. Con este texto, Gutiérrez pone en evidencia las estrechas relaciones que existen entre los movimientos de la sociedad civil latinoamericana con los movimientos globales.

Domingo Lechón con el texto "Snowden nació en la selva Lacandona: reflexiones sobre tecnopolítica y bienes comunes" quiere situar Internet en el conjunto de los bienes comunes. La discusión sobre el procomún, "aquello que nos pertenece a todos y a la vez a nadie", como

lo define Antonio Lafuente sale a relucir cuando está en riesgo. Lechón traza una ruta para conectar dos eventos que pueden parecer dispersos, pero que se encuentran en realidad entretejidos: el movimiento zapatista y Snowden. Defiende la tecnopolítica como opción para defender la red, pero también otros modos alternativos de ser, estar y sentir en el mundo.

En "Participación ciudadana y cultura digital en Brasil" Rodrigo Savazoni realiza un análisis del contexto actual de Brasil, comenta las iniciativas ciudadanas de cambio social y discute sobre las posibilidades de una innovación desde los márgenes, que no pierda su conexión con las raíces, con la cultura popular, lo ancestral. A pesar de la difícil coyuntura para la acción colectiva en el momento de Brasil, la cultura digital puede contribuir a la apertura de espacios de confluencia para los saberes colectivos.

Conclusión

A través de las discusiones propuestas en este monográfico, hemos buscado centrar la atención en el hecho de que a medida que los sistemas de vigilancia crecen y se consolidan en la región, la acción colectiva debe contemplar estrategias integrales y sistemáticas que aborden la multidimensionalidad de esta problemática. Las estrategias deben incorporar la demanda de transparencia y rendición de cuentas, la documentación de las capacidades de vigilancia de los Estados, el análisis técnico de los equipos intervenidos, las estrategias personales y colectivas de defensa digital, la construcción de narrativas que permitan contrarrestar los discursos oficiales sobre la seguridad, la toma de conciencia sobre el derecho a la privacidad, el impulso a iniciativas políticas y jurídicas que garanticen el respeto a los derechos, el desarrollo de propuestas estéticas y técnicas contra la vigilancia.

En el contexto global de vigilancia selectiva y masiva son necesarios los esfuerzos ciudadanos destinados a promover la defensa de Internet como procomún, libre, abierto y neutral, y la soberanía tecnológica como un principio de autonomía necesario para poder construir mundos alternativos. Además, es preciso demandar que la vigilancia se ajuste a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones (2013) con las respectivas salvaguardas. Por eso,en los procesos de acción colectiva adquiere especial relevancia la conformación de redes nacionales, regionales y globales que permitan avanzar en la discusión y la defensa de derechos.

Las distintas visiones y contextos presentados en el monográfico permiten constatar la complejidad y la dificultad para ofrecer respuestas generales.. Dado el carácter supranacional de los sistemas de vigilancia, las soluciones deben construirse en la continuidad entre lo local y lo global. De igual manera, la comprensión acerca de la privacidad debe ser trabajada colectivamente como una construcción social.

Abordar la vigilancia desde sus múltiples dimensiones implica también la búsqueda de marcos de referencia que permitan a los sujetos apropiarse de herramientas técnicas, jurídicas y discursivas como fundamento para sus estrategias de resistencia. Por ello, buscamos inscribir la discusión tanto en una perspectiva macrosocial -como parte de un modelo económico, social y político global- hasta microsocial, que involucra las propias necesidades, percepciones, afectos y decisiones de los sujetos de la vigilancia. Agradecemos a los autores sus contribuciones a este debate.

Referencias

AGAMBEN, G. (2005). *Estado de excepción. Homo Sacer II*. Buenos Aires: Adriana Hidalgo Editora.

ASSANGE, J., APPELBAUM, J., MULLER-MAGUHN, A., y ZIMMERMANN, J. (2012). *Cypherpunks: Freedom and the Future of the Internet*. New York and London: OR Books.

BAUMAN, Z. (1988). Freedom. Minneapolis: University of Minnesota Press.

BAUMAN, Z. y LYON, D.. (2013). *Liquid Surveillance*. Cambridge: Cambridge University Press.

BOGARD, W. (1996). *The simulation of surveillance: Hypercontrol in telematic societies*. Cambridge: Cambridge University Press.

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

CLARKE, R. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498-512.

CITIZEN LAB (2014, 17 de febrero). Mapping Hacking Team's "Untraceable" Spyware. University of Toronto. Recuperado de: <https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/>

CITIZEN LAB (2015, 15 de octubre). Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation. Universtiy of Toronto. Recuperado de: <https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/>

CONTINGENTEMX (2014, 3 de marzo). Spyware de la empresa Hacking Team opera bajo redes mexicanas. Recuperado de: <http://contingentemx.wordpress.com/2014/03/03/spyware-de-la-empresa-hacking-team-opera-bajo-redes-mexicanas/>

CONTINGENTEMX (2015, 22 de octubre). Las pasarelas de la industria de la vigilancia y su relación con los gobiernos mexicanos: escenarios 2015. Recuperado de: <http://contingentemx.net/2015/10/22/las-pasarelas-de-la-industria-de-la-vigilancia-y-su-relacion-con-los-gobiernos-mexicanos-escenarios-2015/>

CRITICAL ART ENSEMBLE (2001). Electronic Civil Disobedience,Simulation, and the Public Sphere. In *Digital Resistance: Explorations in Tactical Media*. New York: Autonomedia. Recuperado de:

<http://www.critical-art.net/books/digital/tact1.pdf>

Deleuze, G. (1992). What is a Dispositif? In Armstrong, T.J. (Ed). *Michel Foucault Philosopher*. Hemel Hempstead: Harvester Wheatsheaf, pp. 159-168.

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

Foucault, M. (2006). *Seguridad, territorio, población*. Buenos Aires: Fondo de cultura económica.

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

Giddens, A. (1987). *The Nation-State and Violence: A Contemporary Critique of Historical Materialism, volume II*. Berkeley: University of California Press.

HackingTeam (s/f). Galileo. Remote control system. [dosier]. Recuperado el 30 de noviembre de 2015 de:
<http://www.hackingteam.it/images/stories/galileo.pdf>

Haggerty, K.D., y Ericson, R.V. (2000). *The surveillant assemblage*. The British Journal of Sociology, 51(4), 605-622.

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

Lyon, D. (2006). 9/11, Synopticon, and Scopophilia: Watching and being watched. *The new politics of surveillance and visibility*, 35-54.

Mathieson, T. (1997). *The Viewer Society*. Theoretical Criminology, 1(2).

Moulier-Boutang, Y. (2011). *Cognitive capitalism*. Cambridge: Polity Press.

Ricaurte, 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.

Rhizomatica (2015, 11 de noviembre). La red autónoma. Boletín informativo, 1. Recuperado de:
<http://rhizomatica.org/2015/11/11/la-red-autonoma-a-bulletin-ofbyfor-our-networks-of-networks/>

Rodríguez, K. (2015). A raíz de la filtración de Hacking Team, EFF y grupos de la sociedad civil en Latinoamérica hacen un llamado por mayores salvaguardas respecto a las tecnologías de vigilancia. *Electronic Frontier Foundation Blog*. Recuperado de:
<https://www.eff.org/node/86768>

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

SIMON, B. (2002). The return of panopticism: Supervision, subjection and the new surveillance. *Surveillance & Society*, 3(1).

WIKILEAKS. (2015, 8 de julio). Hacking Team. Recuperado de: <https://wikileaks.org/hackingteam/emails/>