revista f@ro

Vol. 1. N°27 (I Semestre 2018) – Foro Científico
Págs. 35 a 59
Facultad de Ciencias Sociales, Universidad de Playa Ancha
Valparaíso, Chile | e-ISSN 0718-4018
http://www.revistafaro.cl

Un fantasma recorre la web. Aproximación crítica al trabajo digital y cibervigilancia‡

A spectre is haunting the Web. Critical approach to digital labour and cyber-surveillance

Jorge Valdebenito Allendes§
Universidad de Valparaíso
jorge.valdebenito.allendes@gmail.com

Recibido: 06 de Febrero de 2018
Aceptado: 06 de Julio de 2018

Resumen • El objetivo del presente trabajo es introducir al debate entre el tecno-entusiasmo y el tecno-escepticismo, y la necesidad que esto implica a la hora de formular estrategias de intervención que lidien con problemas vinculados a Internet. Se sostiene una hipótesis doble: que Internet, como red de circulación de información, refleja las dinámicas de explotación propias de la economía global capitalista; y que pensarla como espacio de libertad, constituye una mitificación de esta en omisión del contexto general de lucha de clases que la configura y da soporte. Nociones como las de "prosumidor" y "trabajo digital" permiten entender la concatenación y características de los distintos procesos presentes en la cadena de valor de la industria de hardware y software, vital

‡ El autor agradece especialmente las contribuciones de Melissa Steda, Iván Rivera y Rocío Knipp.
§ Doctorando en Estudios Interdisciplinarios de la Universidad de Valparaíso.

para su funcionamiento. De tal modo, la consideración sobre problemas como ciberamenazas no puede realizarse desde fetiches tecno-céntricos, sino mediante un análisis de sus funciones en cuanto a niveles y procesos partes de una economía política digital extendida globalmente. Las conclusiones indican que Internet expresa contradicciones propias del régimen de producción capitalista, y se invita a la discusión sobre las tácticas que podrían articularse ante ellas.

Palabras clave • Internet, trabajo digital, cibervigilancia, capitalismo digital, explotación.

Abstract • This paper aims to introduce the debate between techno-enthusiasm and techno-skepticism, and the need that this implies when formulating intervention strategies that deal with problems such as privacy on the Internet. A twofold hypothesis is held: that the Internet, as a network of circulation of information, reflects the dynamics of exploitation of the global capitalist economy; and that to think of it as a space of freedom constitutes a mythification based on the omission of the general context of class struggle that configures and supports it. Notions such as those of prosumer and digital work allow us to understand the concatenation and characteristics of the different processes involved in the value chain of the hardware and software industry vital for its operation. Thus, the consideration of elements such as cyber threats cannot spring from pessimistic or enthusiastic technocentric fetishes, but from an extensive analysis of its functions in terms of levels and processes part of a globalized digital political economy. The paper concludes that the Internet expresses global contradictions of its own capitalist systems of production.

Key Words • Internet, digital labour, cyber surveillance, digital capitalism, exploitation.

1. Introducción

Las transformaciones asociadas a la masiva adopción de dispositivos inteligentes en el mundo actual plantean una serie de desafíos altamente complejos en su estudio e intervención (Holt, 2012; Das y Nayak, 2013; Amaro, 2016; Kailemia, 2016). Internet, en tanto red de circulación de información, no puede ser entendida como elemento abstraído de las lógicas que operan sobre los fenómenos constitutivos de la realidad concreta, sino como reflejo o extensión de ellos (Fuchs y Trottier, 2017). Si bien existen vulnerabilidades que son propias de su infraestructura, estas no son fetichizadas tecnocéntricamente, sino que son estudiadas a partir del modo en que son explotadas en un contexto económico y político general. En dicho proceso se involucran tantos actores como usuarios de Internet existen, resumidos en gobiernos, corporaciones y sociedad civil (Kurbalija, 2016). Pese a que el diseño de la red de redes se ha desarrollado en un proceso en el que se distinguen ciertos intereses clave que configuran su código técnico (Feenberg, 2005), no se le debe esencializar positiva o negativamente, sino que se debe estudiar como parte de una totalidad histórica, económica, política y cultural.

Internet se puede entender como una herramienta que evidencia diferentes contradicciones en su uso. Por ejemplo, el problema de la vigilancia masiva sobre la población, y el lucro derivado de la explotación de los datos producidos por millones de internautas (Bigo, 2015; Fuchs y Trottier, 2017). Datos que son apropiados y explotados por corporaciones de diferentes industrias —publicitaria y tecnológica principalmente— transformándolos en información dotada de valor comercial y financiero (Fuchs, 2014a: 74-152). En base a la plusvalía derivada del trabajo digital, compañías como Facebook o Google se enriquecen en base a la especulación realizada sobre los datos recolectados de sus usuarios, conformando una estructura de clases entre propietarios de plataformas y proletariados digitales no reconocidos como tal, este problema se entiende como extensión de dinámicas de explotación propias del mundo offline (Graham, Hjorth y Lehdonvirta, 2017).

De igual modo, prácticas como robos bancarios cometidos por delincuentes informáticos constituyen una mera extensión de lógicas de funcionamiento del mundo offline, y no fenómenos originados por la red de redes. El ciberdelito, por lo tanto, no corresponde esencialmente a algo nuevo y, tal como en el mundo fuera de línea, justifica la introducción de sofisticados sistemas de cibervigilancia (Holt, 2012; Hintz, 2014). La infraestructura de Internet, controlada por gobiernos y corporaciones, además de monitorear todas y cada una de las acciones realizadas por los usuarios de la red, cumple una función política de control y económica de explotación (Fuchs, 2014a). La crítica ante ello, proveniente desde el panopticismo, indica que la gestión de la infraestructura técnica de Internet es formulada y empleada con propósitos de control biopolítico (Foucault, 2006; Caluya, 2010). Pero en el fondo, lo que justifica la introducción de millonarias inversiones en su perfeccionamiento deriva de los beneficios económicos (comerciales y financieros) percibidos por corporaciones de la industria digital (Scholz, 2013; Fuchs y Fisher, 2015).

La respuesta orquestada desde ciertos sectores de la sociedad civil ante ello ha sido articulada acudiendo a valores culturales individualistas y políticos democráticos (Jenkins, 2008; Castells, 2012; Murthy, 2013; Tufekci, 2017). Por ejemplo, demandas por privacidad y transparencia en línea expresan sus limitaciones en no englobar adecuadamente la complejidad que el fenómeno implica desde su origen hasta la configuración de su actualidad. Dicho de otro modo, de reducirse a una cuestión basada puramente en la protección del anonimato en Internet, los intentos de intervención serán limitados. La deep web, así como diferentes técnicas criptográficas, permiten conservar el anonimato en Internet (Bautista, 2015; EFF, 2015); pero el problema no se reduce a ello, sino a todas las condiciones de precariedad y explotación situadas en los distintos procesos productivos de la cadena de valor de la industria digital (Fuchs, 2014a; Bautista, 2015).

La infraestructura de Internet se configura a partir de una compleja y enorme red de servidores, cables submarinos, antenas, satélites, entre otros. La cadena de producción involucra diversos procesos de explotación

medioambiental y de mano de obra, entre las que se encuentran industrias extractivas de minerales como cobalto, litio y oro, y de fabricación en compañías como Foxconn (Manzerolle y Kjosen, 2012; Qiu, Gregg y Crawford, 2014), conocida por sus deplorables condiciones de trabajo, millonarias ganancias que aumentan año a año y gigantescos clientes directos como Apple, Microsoft o Samsung. Sus instalaciones juegan un rol fundamental en la demanda tecnológica contemporánea. Si a lo anterior se agregan los procesos de desecho acelerado por obsolescencias programadas y su daño ambiental, se ilustran las contradicciones internas de los procesos de valorización y acumulación de una economía de capitalismo digital (Chen, 2016). Operando desde la base de un régimen altamente globalizado en el que gobiernos compiten por atraer inversión extranjera abaratando costos laborales y medioambientales de producción, la precarización de estos parece ser la tendencia mundial de todo proceso productivo.

Pero el capital encuentra formas de explotación y apropiación de ganancias no sólo a partir de las fuerzas productivas, sino también desde la mercancía donde se originan términos como el de prosumidor o de consumidor productivo como parte de una economía digital extendida globalmente (Islas-Carmona, 2008; Fuchs y Sevignani, 2013; Kostakis y Giotitsas, 2014; Fuchs y Fisher, 2015). La gestión de la infraestructura de Internet, debido a sus altos costos de instalación y mantenimiento bajo el orden actual, es propiedad de las mismas corporaciones propietarias del tráfico de la red. Compañías como AT&T y Google establecen un oligopolio de la red, ante el que gobiernos y otras instituciones regulatorias adhieren mediante diferentes estrategias de cooperación (Cepal, 2016; Bates, Bavitz y Hessekiel, 2017). Guiados por la superación de brechas digitales y de desarrollo de infraestructura de telecomunicaciones a nivel territorial, terminan reproduciendo las lógicas de explotación y acumulación que las sustentan.

Pero agencias de seguridad gubernamental también explotan sus propios beneficios. Además de la explotación derivada del control del tráfico de datos por parte de corporaciones, se han identificado diferentes tácticas

como la weaponization en contextos generales de ciberguerra (Waltzman, 2017). Dicha práctica convierte ordenadores, mediante exploits u otros malwares, en armas para la ejecución de tácticas de ciberguerra, ciberdelito o ciberterrorismo, ejemplificando la fragilidad en las distintas fases de la edificación de este sistema sociotécnico (Kaspersky, 2017). Ahora bien, esto no debe conducir a la generación de un fetiche esencialista ni determinista de Internet en un sentido positivo o negativo. Internet no es por sí mismo explotación, vigilancia o libertad (Caluya, 2010; Castells, 2012; Scholz, 2013; Fuchs, 2017). La traducción práctica de esta idea es que, tanto diagnósticos como intervenciones realizadas sobre los problemas dados en el funcionamiento de Internet, no se pueden centrar en la cosa en sí. Ello significaría un reduccionismo inadecuado para abordar tanto los desafíos conceptuales de su delimitación como las prácticas para la solución de sus problemas.

A un fenómeno multidimensional - como lo es la configuración y funcionamiento de Internet - se debe aplicar un análisis que articule a lo menos tres dimensiones o niveles fundamentales. El primero de ellos, y que posee cierta centralidad respecto de los dos siguientes, corresponde al económico y, en específico, a las distinciones acerca de los distintos procesos de valorización que ocurren en Internet (Manzerolle y Kjosen, 2012; Marcus y Joseph, 2015; Fuchs y Fisher, 2015). Le sigue el político, en el que se despliegan diferentes tácticas orientadas a consolidar un aparato institucional y jurídico encargado de normalizar el curso de las actividades del nivel económico. Finalmente, se encuentra el cultural en el que se comprenden todos los procesos propios de la configuración de un sistema de creencias, valoraciones, representaciones e/o imaginarios, desde los cuales se legitima la ordenación de los dos primeros. Las discusiones relativas a problemas derivados de la existencia de ciberamenazas deben considerar tales elementos de contexto para lograr su adecuada delimitación.

A continuación, se examina brevemente el debate entre tecno-entusiasmo y tecno-escepticismo desde una perspectiva crítica, especialmente sobre la fetichización que la primera postura realiza de Internet. Luego, se

destaca la necesidad de su comprensión a fin de pensar tácticas de intervención para el funcionamiento de Internet. La relevancia de ello radica en que usualmente las alternativas que formulan estrategias de protección de los "usuarios" de la red omiten aspectos económicos, políticos y culturales de fondo (Fuchs, 2017). Promoviendo, por ejemplo, derechos de privacidad basados en valores neoliberales de responsabilidad individual y/o de participación en espacios democráticos. La limitación de estos es que al ignorar las condiciones de explotación que dan soporte a Internet, sus propuestas no permiten terminar con su problema de base: la monopolización de la infraestructura y del tráfico de datos de la red (Thatcher, O'Sullivan y Mahmoundi, 2016).

Elementos como ciberamenazas deben comprenderse desde una economía política digital por sobre concepciones tecnocéntricas, pesimistas o entusiastas. El potencial de ello es caracterizar las funciones que cumplen ciertas prácticas englobadas en nociones como ciberterrorismo, ciberdelitos, o cibervigilancia en procesos de valorización, de conformación de estructuras regulatorias, o de promoción de principios valóricos, imaginarios, creencias o representaciones. En dicho sentido, la hipótesis del presente trabajo sostiene que Internet como red de circulación de información, refleja las dinámicas de explotación propias de la economía capitalista global (Islas-Carmona, 2008; Scholz, 2013; Fuchs y Fisher, 2015; Graham, Hjorth y Lehdonvirta, 2017). Por lo tanto, pensarla como espacio de libertad constituye una mitificación de esta, y la omisión del contexto general de lucha de clases que la configura y da soporte. No basta entonces con la promoción de acciones contrarias a los usos corporativos y gubernamentales de datos personales que vulneren la privacidad de los individuos, sino con ir al origen mismo del problema con un propósito revolucionario.

2. Procesos, cadenas y valores en Internet: entre tecno-entusiasmo y tecno-escepticismo.

La rápida expansión global de Internet y su penetración en la cotidianidad del orden mundial ha generado un debate que es posible resumir entre dos

posturas: el tecno-entusiasmo y el tecno-escepticismo. Aun cuando cada una posee cierta heterogeneidad interna, la primera se caracteriza por la frecuente defensa del potencial democrático que significa la conformación de un escenario altamente tecnologizado en la era actual (Murthy, 2013; Tufekci, 2017). Por ejemplo, las tecnologías de información y de las comunicaciones (en adelante TICS) permiten empoderar a la ciudadanía en la difusión de abusos e injusticias que sufra por parte de los poderosos. Favoreciendo la libertad de expresión se pueden rastrear hitos clave en el uso realizado de dispositivos móviles y redes sociales de Internet durante las Primaveras Árabes como episodio revolucionario (Castells, 2012; La Tuerka, 2015).

La crítica fundada desde el tecno-escepticismo apunta a develar los fetiches tecnológicos y la omisión de las variables estructurales de contexto que usualmente sostienen argumentos tecno-entusiastas (Fuchs y Sevignani, 2013). La conformación de un escenario globalmente integrado debe entenderse desde una perspectiva histórica y no puramente técnica. Ello permite problematizar el hilo de las decisiones políticas y económicas realizadas en torno a la inversión en desarrollo tecnológico. Al examinar con detención, muchas de ellas se enmarcan en el transcurso de diferentes tipos de conflictos comerciales, bélicos o sociales (Fuchs y Trottier, 2017). Si se presta especial atención a cuestiones prácticas de acceso y dominio tecnológico en la sociedad es posible identificar la progresión de diferentes dinámicas de exclusión generadas en torno al dominio técnico, y no al revés; expresadas en muchos casos, además, en el fortalecimiento de asimetrías de poder en términos geográficos (Marcus y Joseph, 2015).

El desarrollo técnico, bajo las condiciones de producción globales y contemporáneas, exhibe en la práctica una orientación hacia la contribución de la acumulación de capital por parte de quienes lo comandan (Manzerolle y Kjosen, 2012). Como parte de ciclos de producción económica, este parece colaborar más con el enriquecimiento de las corporaciones de la industria tecnológica que lo dirige por sobre la emancipación de los oprimidos del mundo. Pese a que se ha explorado en diversas investigaciones el vínculo entre el uso de redes sociales de Internet

y ciclos de movilización ciudadana (Murthy, 2013; Tufekci, 2017), este no está exento de contradicciones (Fuchs, 2014b). En primer lugar, las movilizaciones sociales poseen una trayectoria que, si bien contiene cierta relación histórica con el desarrollo de medios técnicos de producción, distribución y circulación de información, no es estrictamente causal. Pareciera ser que su surgimiento responde más bien a la agudización de diferentes cuestiones políticas, como crisis de legitimidad de un sistema político, o económicas, como abruptas inequidades materiales en un país determinado.

A lo anterior se suman las denominadas brechas digitales referidas a la distribución desigual en el uso y manejo de recursos como TICS en la sociedad, posibles de describir siguiendo variables como edad, nivel educacional, zona de residencia (urbana o rural), entre otras. Constituye una limitación reconocida incluso por tecnoentusiastas (Cepal, 2016; Murthy, 2013). Suponer que la ciudadanía se configura en base a una distribución equitativa de recursos es un error puesto que la masificación del uso de TICS se traduce, en muchos casos, en la generación de nuevas asimetrías sociales. Esto constituye un arma de doble filo: empodera a quienes se familiarizan con ellas y discrimina a aquellos que no (Fuchs, 2014b).

Lo tecnológico, entendido desde una globalidad económica digital y distinciones tecno-escépticas, instala la duda acerca de si acaso es tan beneficioso como se plantea por el tecno-entusiasmo. Hechos englobados por ellas corresponden básicamente a dos. En primer lugar, la generación y reproducción de nuevas asimetrías al interior de la sociedad, en base a las inequidades de dominio o habilidades técnicas de los sujetos. Segundo, el beneficio corporativo y gubernamental en cuanto a explotación y vigilancia, derivado de la penetración de diferentes TICS, principalmente de aquellas smart (Thatcher et al., 2016). De tal modo, la valoración de lo digital como condición de posibilidad y realización del empoderamiento y/o emancipación se fundaría en un fetiche tecnológico, que además terminaría reproduciendo dominaciones de clase en base a la propiedad

de los medios de producción tecnológica y digital (Fuchs, 2014a; Marx y Engels, 2017)

El tecno-optimismo representa, en resumen, un idealismo en vista de la omisión de las condiciones materiales que contextualizan el diseño y desarrollo de nuevas tecnologías. Igualmente es imposible entender el desarrollo tecnológico en su complejidad si se le piensa únicamente en términos técnicos (Adorno y Horkheimer, 1998). Nociones como las de 'código técnico' permiten examinar la naturalización técnica que se realiza de ciertos requisitos que ocultan en realidad propósitos culturales, económicos y/o políticos (Feenberg, 2005). Ejemplos de ello pueden encontrarse en la configuración técnica de los smartphones, dotados hoy en día de dos cámaras web, tres micrófonos, sistemas de geolocalización GPS, y una vida útil que no supera los tres años. Es innegable que la comunicación es indispensable para la ciudadanía, sea en contextos de catástrofe o de movilización social, pero ¿qué sucede cuando el diseño del hardware permite la implementación de tácticas opresivas por parte de agentes de seguridad del Estado?.

Desde este debate es posible entender que Internet se encuentra lejos de ser un medio colectivo de producción y circulación de información, sino que es diseñado, configurado y operado por agentes específicos como gobiernos y corporaciones. De hecho, las capas que conforman su arquitectura son propiedad de grandes corporaciones y consorcios internacionales, entre las que figuran compañías como Google, AT&T, y Facebook (Marcus y Joseph, 2015). Las que precisamente poseen la red de cables submarinos mediante los cuales fluye la información, o los balones de helio, propiedad de Google, que proveen de conexión wi-fi a lugares remotos y proyectos de cables específicos como Tannat y Monet. Por cuestiones de costo e inversión asociadas a la instalación, mantenimiento y actualización de lo que constituye finalmente la espina dorsal del Internet, resulta asunto exclusivo para agentes con capacidad de inversión de grandes capitales. Esto configura en la práctica un sistema altamente monopolizado en el que las mismas compañías propietarias de la

infraestructura son las que controlan el tráfico de datos (Thatcher et al, 2016).

Tales elementos difícilmente permiten sostener que Internet es sinónimo de libertad o emancipación social (Castells, 2012; Murthy, 2013; La Tuerka, 2015). Rastreando elementos fundamentales de su composición se hallan contradicciones presentes en diferentes niveles. La instalación de macrosistemas técnicos compuestos a partir de cables, servidores, antenas, entre otros, responde a decisiones que van más allá de parámetros técnicos (Feenberg, 2005). Interseccionadas con aspectos políticos y económicos, son recubiertas usualmente con discursos de inclusión y reducción de brechas digitales (Bates et al, 2017). El tecno-escepticismo permite enfatizar, al mismo tiempo, en los sucesos que marcan la gestión de acuerdos de cooperación intersectorial entre gobiernos y corporaciones.

Así, la constitución de un orden jurídico e institucional se realiza acorde al sostenimiento de procesos de producción y acumulación de datos tendientes a su explotación y valorización bajo lógicas comerciales y financieras capitalistas (Scholz, 2013; Fuchs y Fisher, 2015). Es el lucro derivado de los usos de la información producida por prosumidores en dispositivos de su manufactura, operados en sus servidores y bajo sus licencias de software en colaboración con organismos regulatorios, lo que conforma esta gran economía digital (Islas-Carmona, 2008; Graham et al, 2017). Innovación, manejo de información y su posterior financiarización en bolsas de valores, conforman la puesta en marcha de un modelo de negocios basado en una economía de capitalismo digital. En tal aspecto se deben reconocer los intentos por implementar una economía política basada en criptomonedas como los bitcoins. No obstante, y pese a basarse en Comunes, más que brindar soluciones a los debates sobre la crisis financiera, plantea interrogantes pertinentes de abordar una vez resuelto aspectos fundamentales de los intermediarios y propietarios de la circulación de información en Internet (Kostakis y Giotitsas, 2014).

Tampoco es posible afirmar que Internet permite superar las inequidades socioeconómicas del mundo offline, por el contrario, al operar bajo lógicas

comercial-financieras de producción y acumulación (Fuchs, 2014a) las potencialidades que este entrega se restringe a segmentos con capacidad adquisitiva, contraviniendo discursos pro-inclusión y democratización de la red (Marcus y Joseph, 2015). Más aún, en la cadena de producción propia de dispositivos e insumos necesarios para su uso se encuentran grandes multinacionales de la industria manufacturera de hardwares y softwares. Contrario a la apreciación positiva que se pudiera tener de estas, se caracterizan, en general, por poseer regímenes laborales de alta precariedad (Qiu et al., 2014). Foxconn, corporación taiwanesa y principal fabricante de componentes electrónicos, constituye su ejemplo por antonomasia. Con trabajadores suicidas que protestan por mejores condiciones laborales, clientes de renombre como Apple y Microsoft, y exuberantes ganancias lucrativas, ilustra patentemente las contradicciones internas del modo de producción capitalista en la industria tecnológica (Fuchs, 2014a).

La procedencia de materias primas necesarias para la manufactura de dispositivos como teléfonos, computadores, o tablets, así como su posterior desecho, involucra también condiciones de rápido deterioro humano y medioambiental (Chen, 2016). Distinguible a partir de sucesos propios de la lógica extractivista presente en la industria minera de litio, cobalto y oro situada en el tercer mundo, ha implicado un alto costo a países africanos como el Congo (Qiu et al., 2014: 574-575). La demanda de materias prima aumenta en la medida que aparatos electrónicos son crecientemente requeridos por el mercado, lo que se traduce, además, en la generación de toneladas de chatarra tecnológica. En tal sentido, si se consideran, por ejemplo, los diseños que contienen desarrollos que hablan de una obsolescencia programada, la situación empeora aún más.

En el caso de la industria de softwares la precariedad y exclusión es vivida por desarrolladores de compañías de la India y Silicon Valley (Fuchs, 2014a): Exigencia desmesurada, jornadas laborales que no dan espacio a descansos, despiadada competitividad entre empleados terminan por ocasionar en muchos de sus trabajadores de cuello blanco síndromes de burnout. Ahora bien, en el caso de la mano de obra de cuello azul, las

labores de limpieza, mantenimiento de maquinaria y manipulación de objetos tóxicos, entre otras, son realizadas principalmente por mujeres y/o migrantes. Disfunciones respiratorias que van desde la silicosis al cáncer del pulmón, enfermedades a la piel, abortos espontáneos, y enfermedades congénitas expresan la reproducción de una economía política del trabajo racista y sexista que mutila trabajadores, destruye familias y el ecosistema (Fuchs, 2014a: 231; Qiu et al., 2014).

En consideración de los procesos involucrados en la configuración y manufactura de requerimientos necesarios para el uso de Internet ¿puede sostenerse que es sinónimo de libertad? Castells, a raíz de los acontecimientos de las Primaveras Árabes, divulga tal interpretación (Castells, 2012; La Tuerka, 2015; Tufekci, 2017), por lo que es necesario considerarla desde aspectos propios que configuran el funcionamiento de los procesos de movilización social. Primeramente, es difícil sostener que estos se encuentran determinados por la disponibilidad de TICS para quienes los ejecutan. Su lectura de los actos de censura gubernamental sobre Internet en el transcurso de las Primaveras Árabes sostiene que ante tal amenaza al ejercicio de libertades civiles se generó una efervescencia de masas (Murthy, 2013; Ocaña, 2015). Violentos enfrentamientos entre civiles y fuerzas de orden público, intervención de la comunidad internacional, y derrocamiento de regímenes dictatoriales fueron consecuencias de tales acontecimientos.

No obstante, la respuesta desde el tecno-escepticismo esbozada por Christian Fuchs (2014b) disecciona tal argumento. Su conclusión indica que las Primaveras Árabes no pueden ser entendidas en omisión de las condiciones históricas y estructurales en las que se sitúan (Ocaña, 2015; Fuchs y Trottier, 2017). Su explicación enfatiza en las altas desigualdades económicas propias de los países de oriente medio, la existencia de un sistema político autoritario y centralizado, y la propagación de valores liberales de democracia y libertad. Sin caer en romanticismos de suma de factores (Lenin, 2014), tales elementos deben articular una explicación realista sobre lo ocurrido, por sobre idealismos fundados en fetiches tecnológicos. Más aún cuando las condiciones sobre las que opera la

propiedad de la infraestructura ha contribuido a la generación de nuevas y perfeccionadas formas de control social cimentadas en la red de redes (Manzerolle y Kjosen, 2012; Marcus y Joseph, 2015; Thatcher et al, 2016). Se trata de la cibervigilancia, la cual se comprende como parte de un complejo entramado de ciberamenazas para los usuarios de Internet, sobre las que se profundiza a continuación.

3. Aproximación a amenazas y seguridad en Internet

El concepto de ciberamenazas remite a un conjunto heterogéneo y cambiante de riesgos existentes en la red, partes de un proceso de expansión y consolidación de una economía digital de carácter global (Amaro, 2016; Bates et al, 2017; Graham et al, 2017). El aumento de la cantidad de internautas, la cantidad de tiempo que estos permanecen conectados a Internet, y dispositivos de los que cada uno dispone, es manifestación del sostenido crecimiento de su productividad. La penetración de Internet se ha dado en diferentes áreas sociales y comerciales que van desde actividades lúdico recreativas, operaciones financieras y gestión de sistemas fundamentales para el funcionamiento de una ciudad, hasta transporte o energía. Esto es problemático a la hora de considerar la vulnerabilidad propia de los sistemas informáticos que ha involucrado igualmente una extensión de los límites de la actividad delictual, originando diferentes repertorios de ciberdelitos (Oxman, 2013; Das y Nayak, 2013).

Phising, pharming, robos a particulares mediante adulteración de cuentas bancarias, tráfico de armas, estupefacientes y/o pornografía, son algunos repertorios de los denominados ciberdelitos. Casos específicos se pueden encontrar, por ejemplo, en la vulneración del sistema de seguridad del Banco Central de Bangladesh en el año 2016, operado por el grupo Lazarus (Evan, Leverett, Ruffle, Coburn, Bourdeau, Gunaratna y Ralph, 2017). Con un motín de US$81 millones, sus acciones como las de tantos otros grupos similares se han replicado en diferentes ámbitos, como de industrias de medios o manufactureras. La evolución de amenazas como estas, además de la introducción de nuevos virus y malwares aumenta a ritmos

exponenciales. En 1994 se hablaba de la generación diaria de un nuevo virus, cifra que para el 2017 aumentó a 323.000 malwares diarios (Kaspersky, 2017).

Su importancia reside en que el rango de sucesos de acciones ciberdelictuales involucra igualmente ataques a las denominadas infraestructuras críticas (Masera y Ortíz, 2015). Comprendiendo aquellas redes de sistemas físicos y virtuales vitales para el funcionamiento de un país. Se destacan entre ellas instalaciones de servicios de emergencia, salud, agua, energía eléctrica, gasoductos, transporte, agricultura, financieros, comerciales, defensa, químicas, comunicación e información, entre otros. No existe certeza sobre las eventuales consecuencias que tendría la ejecución de un bien planificado ciberataque sobre ellas. Todas ellas son vulnerables en contextos de ciberguerra o de ataques ciberterroristas (Waltzman, 2017). Apagones masivos, descarrilamientos de trenes, descoordinación de vuelos aéreos, destrucción de datos bancarios e, incluso, pérdida de control de sistemas de gestión militar, serían parte de sus repertorios. Ejemplos concretos pueden rastrearse en el sabotaje del sistema de suministro eléctrico a Ucrania en el año 2005, del sistema bancario de Estonia en el año 2007 y del sistema nuclear de Irán mediante el malware Stuxnet (Holt, 2012; Amaro, 2016).

Estos presuponen un manejo técnico por parte de quienes los ejecutan, quienes resguardan su privacidad empleando tácticas de criptografía y protegen el anonimato de sus acciones desde, por ejemplo, la deep web (Bautista, 2015). Dificultando su seguimiento por parte de policías y otros agentes de seguridad ciberdelictual, su existencia nutre el desarrollo de una compleja industria de ciberseguridad. Compañías como Kaspersky o Eset destacan en dicho ámbito, además de las acciones realizadas por diferentes ejércitos mediante sus departamentos de ciberguerra que han reaccionado ante las vulnerabilidades de los sistemas informáticos (Holt, 2012; Kaspersky, 2017). La respuesta de estas se encamina actualmente en implementar procedimientos de monitoreo y mitigación de ciberataques, similar a las estrategias de policías del mundo offline. No obstante, las estimaciones para el año 2016 sobre los costos de sus daños indican un

aproximado de US$400 billones, mientras que la inversión en ciberseguridad marca un aproximado de US$175 billones (Ross, 2016).

Estas acciones no corresponden a la aparición de prácticas o fenómenos nuevos debido a la introducción de nuevas tecnologías informáticas. El delito, el terrorismo, y la guerra poseen una historia muy anterior a ellas y, en dicho sentido, sólo representan expresiones de su actualización en la era digital (Evan et al, 2017; Fuchs y Trottier, 2017). Suponer lo contrario sería caer en fetiches tecno-centristas. Ahora bien, lo que sí podría corresponder a algo relativamente reciente es la entrada de técnicas de vigilancia poblacional masiva desde gobiernos y corporaciones. Pese a los conocidos ejemplos del siglo XX del FBI de John Edgar Hoover, o la Gestapo, y la Stasi, el perfeccionamiento de lo que se entiende hoy por cibervigilancia es algo sin antecedentes (Caluya, 2010; Bigo, 2015). Para su ejecución se desarrollan acuerdos comerciales entre distintos agentes corporativos y gubernamentales como parte de una economía política de la vigilancia, entre propietarios de la infraestructura y de los sistemas regulatorios vigentes (Hintz, 2014; Fuchs, 2014a: 85-122).

Mediáticamente, podría decirse que la atención sobre estos asuntos se debe en parte a las divulgaciones realizadas por Julian Assange y Edward Snowden (Ocaña, 2015; Fuchs y Trottier, 2017). Ello ha contribuido a la popularización de ciertas iniciativas que sostienen que Internet, uno de los más grandes inventos de la humanidad, sería, pese a todo, un facilitador del totalitarismo. Sistemas como Echelon, Prism, Xkeyscore, y Tempora, además de la difusión de casos como el de Cambridge Analytica, ilustran tales nociones (Bigo, 2015). El escenario se configura a partir de actores que cumplen funciones específicas en procesos concretos de la conformación de una totalidad económica, política y cultural: las corporaciones se benefician de diferentes procesos de valorización de los datos producidos por los internautas, y, al mismo tiempo, agentes gubernamentales conforman sistemas políticos que permiten la operación de procesos productivos.

En cuanto a la prensa y medios de comunicación, estos colaboran con conformación de un sistema de creencias que desplaza el conflicto de

clases presente en tales procesos. Por el contrario, centran la interpretación en nociones humanitarias y tecno-pesimistas, resolubles mediante fórmulas convencionales de derechos humanos y políticas públicas. Dicha lectura no permite pensar las relaciones sociales de producción presentes en el modo de acumulación capitalista que configura la economía digital contemporánea (Manzerolle y Kjosen, 2012; Qiu et al, 2014).

Así, el panopticismo instala una visión fundada en idealismos que no permiten avanzar en la conformación de programas y tácticas de lucha entre productores y propietarios bajo un esquema de hegemonía capitalista. Por sobre la toma de los medios de producción, promueve ideas como que la gubernamentalidad del poder no es algo que se encuentra centralizado, sino diseminado de manera omnipresente en la sociedad moderna (Foucault, 2006). No obstante, la existencia de los privilegios de unos descansan sobre condiciones de opresión y explotación de otros, siendo este el componente de la lucha de clases esencial para toda iniciativa de transformación social actual (Fuchs, 2014a). De ello no se debe entender que Internet posee una esencia alienante o emancipatoria, en tanto objeto, puede servir para propósitos emancipatorios o reaccionarios. Su problema contemporáneo reside en estar sujeto - como pieza funcional inserta en un modo de producción determinado - a lógicas liberal-burguesas de la propiedad privada (Marx y Engels, 2017: 51-72).

Para el tecno-entusiasmo la cibervigilancia, pese a todo, no es contraria al enunciado de que Internet es un espacio de libertad. "Pese a ser vigilado, no puede ser controlado", señaló Castells en una entrevista televisiva (La Tuerka, 2015). Más allá de la lucha contra el delito, terrorismo, o carreras armamentísticas entre Estados, la construcción de sistemas de cibervigilancia constituye también una promesa de solucionismo técnico en sistemas proclives a modernizarse (Amaro, 2016; Bates et al, 2017; Evan et al, 2017). Sistemas de iluminación, control de tráfico, entre otros, son proclives a la intervención de soluciones smart a sus rendimientos (Manzerolle y Kjosen, 2012; Niaros, 2016; Fuchs y Trottier, 2017). Pero el terrorismo no se detendrá por la introducción de más cámaras de vigilancia en las ciudades, ni el ciberterrorismo por el monitoreo de ciberamenazas,

ya sea por vulnerabilidades internas de la infraestructura o por elementos que la sobrepasan (Kailemia, 2016; Kaspersky, 2017). Igualmente, las soluciones de smart cities han estado lejos de contribuir, por ejemplo, a la eficiencia energética al estar cooptadas por intereses conservadores de gobiernos y corporaciones, engendrando nuevas formas de estigmatización y criminalización espacial (Niaros, 2016; Thatcher et al., 2016).

4. Reflexión final: Privacidad ¿reforma o revolución?

La célebre frase atribuida a Rosa Luxemburgo encierra un enigmático principio: el capitalismo en su desarrollo ha asentado sostenidamente los gérmenes de su propia destrucción. Esta proposición es pertinente de considerar a la hora de examinar las diferentes acciones orientadas a denunciar la violación de derechos de privacidad y vulneración de libertades en Internet por parte de gobiernos y corporaciones hacia la ciudadanía. Exigiendo mayor transparencia en el uso que hacen tales entidades de los análisis que realizan sobre el tráfico de datos, y cláusulas que aseguren la privacidad de los usuarios que los han producido. Derechos de autor, privacidad y de libertad de expresión son parte de las demandas. También hay iniciativas que apuestan por fomentar el uso de herramientas que protejan la privacidad de los usuarios de Internet, basadas en recursos criptográficos como el navegador Tor (EFF, 2015; Jardine, 2016). Tal navegador, utilizando el modelo de redes de encaminamiento de cebolla, permite mantener la privacidad del usuario con respecto a su tráfico en Internet. No exentas de problemas o limitaciones técnicas, actualmente significa una alternativa viable para dificultar el ejercicio de las facultades de los sistemas de cibervigilancia.

Pero cualquier iniciativa que se proponga lidiar con los aspectos que restrinjan el ejercicio de libertades civiles en Internet debe comenzar por dos aspectos fundamentales. El primero trata sobre los aspectos ideológicos que figuran a Internet como un espacio de participación universal y horizontal y, por lo tanto, un aporte para una nueva cultura democrática (Jenkins, 2008; Fuchs, 2014a: 122). El segundo consiste en develar la

apariencia oculta de la explotación usualmente enmascarada como juego o recreación. La noción de web 2.0 suele sustentarse en tales principios, los que se conjugan con fundamentos neoliberales de responsabilidad individual y competitividad (Murthy, 2013; Tufekci, 2017: 189-222).

Sin embargo, ello suele ignorar la relación entre la industria tecnológica y, en específico, aquella basada en la entrega de servicios digitales y el desarrollo de las últimas crisis financieras. La aparición de nuevas plataformas de producción de información personal basadas en valores neoliberales de cultura participativa y de compromiso individual (Jenkins, 2008), en el modo de explotación y en acumulación capitalista se extiende hacia un emergente nicho de publicidad dirigida. Los usuarios, de tal modo, generan el valor mediante la actividad que realizan en tales plataformas, permitiendo a sus propietarios especular en base a la información derivada de ella. Ello significa la realización de la expansión capitalista en todos sus términos: fetichización de las mercancías en cuanto a información "libre y participativa", explotación del trabajo humano en la producción de datos en plataformas de propiedad privada, y composición de una "nueva" estructura de clases entre explotadores y explotados.

Desde lo anterior es posible indagar en los alcances que poseen las alternativas que actualmente se enuncian como reivindicativas de un Internet libre y seguro. Entre algunos de los elementos con los que estas deben lidiar figuran, por ejemplo, la brecha digital, articuladora de una demanda hacia la democratización de la comunicación. Por ejemplo, en América Latina la tasa de acceso a Internet es baja (entre 45% y 55%) en comparación a la realidad europea (entre 80% y 90%) (CEPAL, 2016). De ahí que la penetración de herramientas como Tor u otros mecanismos de seguridad entre los usuarios sea bastante escasa, lo cual asegura el oligopolio de las grandes productoras de hardware y software privado sobre el tráfico de datos circulante en Internet. Esto no implica que los sujetos sin acceso directo a Internet estén liberados de la cibervigilancia. Diferentes dispositivos de seguridad conectados vía "Internet de las cosas" (Sosa y Godoy, 2014: 41-45), como reconocimiento facial, biometría, cámaras, drones, etc., presentes en espacios públicos y semipúblicos,

además de la recolección de datos mediante sistemas de comercio y banca electrónica, transporte, telecomunicaciones, entre otros, operan sobre tal segmento de la población (Niaros, 2016).

Es posible identificar diferentes esfuerzos regulatorios por proteger a los individuos de prácticas que vulneren elementos como su privacidad e integridad en línea. Uno de estos corresponde a la gobernanza de Internet con una estrategia que busca articular principios regulatorios a ser incorporados por los Estados en sus jurisdicciones (Kurbalija, 2016). Pero su lento desarrollo sujeto a diferentes oscilaciones políticas y económicas coyunturales, ha articulado la configuración de nuevos instrumentos más efectivos. Ejemplo de ello es el Reglamento General de Protección de Datos de la Unión Europea, el que acudiendo a diversas áreas de los derechos nacionales se ha implementado recientemente como mecanismo de regulación digital. Derechos de consumidores, derechos civiles, códigos penales e incluso fórmulas de derechos humanos figuran entre ellos.

Instrumentos como los señalados deben lidiar con la limitación de lidiar localmente con problemas globales. Prueba de ello es la secreta ciberguerra extendida mundialmente, en la que estrategias de ciberseguridad militar podría decirse que corresponde a su expresión por antonomasia. La actualización de los planes de defensa e inteligencia de los gobiernos se concibe como parte de estrategias políticas y económicas en un contexto generalizado de guerra extendida mundialmente, pero desarrollada secretamente (Waltzman, 2017). Los actores comunes, prosumidores y/o trabajadores digitales de Internet están llamados por una cuestión de responsabilidad política de clase a responder ante ello de modo revolucionario. En este caso, el problema reside en evitar la colaboración de clases, dada de modo tripartito entre gobiernos, corporaciones y sociedad civil, en desmedro de esta última en tanto masa proletaria de Internet, por ejemplo, en los frentes amplios o populares. Es decir, para aplacar las tendencias globales del capitalismo y su economía mundial, se trata de hacer una política por la revolución mundial. No una querella hacia Estados nacionales, tendiente en el mejor de los casos al

mito del socialismo en un solo país, sino hacia un estado de revolución permanente (Bosch, 2017).

Las condiciones que configuran Internet de modo global contienen las posibilidades de realización para la articulación de demandas con perspectiva internacionalista y de lucha de clases. Esto permitiría enfrentar directamente las barreras que mantienen a Internet diezmado como una mercancía de propiedad corporativa, empleada como pieza fundamental del despliegue de distintos procesos de valorización en una economía capitalista mundial. Fundados en principios de explotación del trabajo humano, se da en condiciones no reconocidas, como es el caso de los prosumidores. Por otra parte, la totalidad de su desarrollo, dado en plataformas digitales, extractivas y manufactureras, condiciona a su vez la configuración de un sistema institucional y regulatorio afín al orden económico. Sustentando mitos jurídicos como el de la regulación nacional y fetiches económicos como el de la autosuficiencia de las economías nacionales, las alternativas de cambio y transformación amortiguan a priori su alcance. Estas últimas, acuden a principios neoliberales de la participación en espacios democráticos y de responsabilidad individual y social-empresarial.

El debate en torno a Internet, por tanto, representa la extensión de un campo de combate conceptual y práctico donde se enfrentan, fundamentalmente, posturas filosófico-económicas de intervención política en la era contemporánea. Entender sus respectivos avances y retrocesos al margen de las dinámicas generales de lucha de clases, constituye una tarea desprovista de contexto histórico, político y social. Fundamental para la elaboración de cualquier programa táctico de transformación, dada la configuración y funcionamiento actual de Internet, es delimitarlo como cuestión de propiedad y acumulación. Los beneficios de las estrategias comerciales y financieras efectuadas sobre la información producida por millones de internautas, así como de sus usos políticos, son parte de un oligopolio corporativo y gubernamental. Desde tal propuesta, se invita al trabajo de diseño de programas con perspectiva "usuaria", que pueden ir desde el control obrero de la ciber-producción, el tele-comunismo de

redes, el establecimiento de una economía digital de comunes, entre otras, y a eventuales combinaciones de niveles entre estas.

Referencias Bibliográficas

Adorno, T., & Horkheimer, M. (1998). Dialéctica de la ilustración. Fragmentos filosóficos. Madrid: Trotta.

Amaro, J. (2016). Seguridad en Internet. Paakat, Revista de Tecnología y Sociedad, 6 (11), 1-9.

Bates, S., Bavitz, C., & Hessekiel, K. (2017). Zero rating & Internet adoption: The role of Telcos, ISPs, & Technology companies in expanding global Internet access. Digital Access to Scholarship at Harvard, 1-13. (Consultado en línea el 24.01.2018). Recovered from http://nrs.harvard.edu/urn-3:HUL.InstRepos:33982356

Bautista, D. (2015). Deep web: Aproximaciones a la ciber irresponsabilidad. Revista Latinoamericana de Bioética, 15 (1), 26-37.

Bigo, D. (2015). Vigilancia electrónica a gran escala y listas de alerta: ¿Productos de una política paranoica? REMHU, 23 (45), 11-42.

Bosch, C. (2017). Los orígenes de la cuarta internacional en argentina. Liborio Justo y el caso del grupo obrero revolucionario y la liga obrera revolucionaria. Diálogos, Revista Electrónica de Historia, 18 (1), 201-226.

Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. Social Studies, 16 (5), 621-633.

Castells, M. (2012). Redes de indignación y esperanza. España: Alianza.

Comisión Económica para América Latina y el Caribe (CEPAL). (2016). Estado de la banda ancha en América Latina y el Caribe 2016. Santiago de Chile: Naciones Unidas.

Chen, S. (2016). The Materialist Circuits and the Quest for Environmental Justice in ICT's Global Expansion. Triple-c, 14 (1), 121-131.

Das, S., & Nayak, T. (2013). Impact of cyber crime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6 (2), 142-153.

EFF (2015). Tor Hidden services, How hidden is "hidden"? (consultado en línea el 9.01.2018). Recovered from https://www.eff.org/files/2015/01/26/20141228-speigel-analytics_on_security_of_tor_hidden_services_0.pdf

Evan, T., Leverett, E., Ruffle, S. J., Coburn, A. W., Bourdeau, J., Gunaratna, R., & Ralph, D. (2017). Cyber Terrorism: Assessment of the Threat to Insurance. Cambridge Risk Framework series. Centre for Risk Studies, University of Cambridge. (Consultado en línea el 6.05.2018). Recovered from https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/pool-re-cyber-terrorism.pdf

Feenberg, A. (2005). Teoría crítica de la tecnología. Revista CTS, 5 (2), 109-123.

Foucault, M. (2006). Seguridad, territorio, población: Curso en el College de France 1977-1978. Buenos Aires: Fondo de Cultura Económica.

Fuchs, C., & Sevignani, S. (2013). What is digital labour? What is digital work? What's their difference? And why these questions matter for understanding social media?. TripleC, 11 (2), 237-293.

Fuchs, C. (2014a). Digital labour and Karl Marx. Londres: Routledge.

Fuchs, C. (2014b). Social media. A critical introduction. Londres: Sage.

Fuchs, C. (2017). Hacia un estudio marxiano de Internet. Revista de ciencias sociales (Cr), 1 (155), 63-89.

Fuchs, C. & Fisher, E. (2015). Reconsidering value and labour in the digital age. Londres: Palgrave Macmillan.

Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden. Journal of Information, Communication & Ethics in Society, 15 (4), 412-444.

Graham, M., Hjorth, I., & Lehdonvirta, V. (2017). Digital labour and development: impacts of global digital labour platforms and the gig economy on worker livelihoods. Transfer, European Review of Labour and Research, 23 (2), 135–162.

Hintz, A. (2014). Outsourcing surveillance - Privatising policy: Communications regulations by commercial intermediaries. Birkbeck Law Review, 2 (2), 349-367.

Holt, T. (2012). Exploring the Intersections of technology, Crime, and Terror. Terrorism and Political Violence, 24 (2), 337-354.

Islas-Carmona, J. O. (2008). El prosumidor. El actor comunicativo de la sociedad de la ubicuidad. Palabra Clave, 11 (1), 29-39.

Jardine, E. (2016). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. New media & society, 20 (2), 1-18.

Jenkins, H. (2008). Convergence culture: La cultura de la convergencia de los medios de comunicación. Barcelona: Paidós.

Kailemia, W. (2016). The spectacle of terrorism: Exploring the impact of "Blind Acting Out" and "Phatic Communication". Journal of Terrorism Research, 7 (2), 91-102.

Kaspersky Lab. (2017). Machine Learning for Malware Detection. (Consultado en línea el 11.05.2018). Recovered from https://media.kaspersky.com/en/enterprise-security/Kaspersky-Lab-Whitepaper-Machine-Learning.pdf

Kostakis, V., & Giotitsas, C. (2014). The (A)Political economy of Bitcoin. Triple-c, 12 (2), 431-440.

Kurbalija, J. (2016). Introducción a la gobernanza de Internet. Malta: DiploFoundation.

La Tuerka. (2015). Otra Vuelta de Tuerka, Pablo Iglesias con Manuel Castells. (Consultado en línea el 20.12.2017).Recovered from https://www.youtube.com/watch?v=dU-MD3NqmQ8

Lenin, V.I. (2014). Para una caracterización del romanticismo económico (Sismondi y nuestros sismondistas nacionales). Marxist.org. Recovered from https://www.marxists.org/espanol/lenin/obras/1897/romanticismo-economico.htm (consultado en línea el 23.05.2018)

Marcus, D., y Joseph, D. (2015). The spatial fix. Triple-c, 13 (2), 223-247.

Manzerolle, V., & Kjosen, A. (2012). The Communication of Capital: Digital Media and the Logic of Acceleration. Triple-C, 10 (2), 214-229.

Marx, K. & Engels, F. (2017). El manifiesto comunista. Buenos Aires: Taurus.

Masera, G. & Ortíz, J. (2015). Gobernanza de riesgos en la sociedad de la información. G. Cuadrado, J. Redmond & R.. López (Eds.). Conceptos y lenguajes en ciencia y tecnología (pp. 361-380). Valparaíso, Chile: Instituto de Filosofía, Universidad de Valparaíso.

Murthy, D. (2013). Social Communication in the Twitter Age (Digital Media and Society). Cambridge: Polity Press.

Niaros, V. (2016). Introducing a Taxonomy of the "Smart City": Towards a Commons-Oriented Approach?. Triple-c, 14 (1), 51-61.

Ocaña, M. (2015). Ciberdisidencias: De la primavera árabe a Snowden. Comunicación y Sociedad, 24, 295-301.

Oxman, N. (2013). Estafas informáticas a través de Internet: Acerca de la imputación penal del "phising" y el "pharming". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, (41), 211-262.

Qiu, J. L., Gregg, M., & Crawford, K. (2014). Circuits of Labour: A Labour Theory of the iPhone Era. Triple-c, 12 (2), 564-581.

Ross, T. (2016). The industries of the future. Nueva York: Simon and Schuster.

Scholz, T. (2013). Digital labour. The Internet as playground and factory. Nueva York y Oxon: Routledge.

Sosa, E. & Godoy, D. (2014). Internet del futuro. Desafíos y perspectivas. Revista Ciencia y Tecnología, 16 (21), 40-46.

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. Environment and Planning D: Society and Space, 34 (6), 990-1006.

Tufekci, Z. (2017). Twitter and tear gas. Estados Unidos: Yale University Press.

Waltzman, R. (2017). The weaponization of information. The need for cognitive security. (Consultado en línea el 12.05.2018). Recovered from https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf