

POSVERDAD, AGNOTOLOGÍA E INSTRUMENTALIDAD EN INTERNET

Rodrigo Iván Liceaga Mendoza*

RESUMEN. En una época de relativización y descrédito por la verdad, como mera opinión o manipulación (*posverdad*), y de un uso deliberado de la producción y manipulación de la ignorancia (*agnostología*) que es crecientemente movilizadado por medios digitales, nula atención se ha prestado a la relación entre estas prácticas y el diseño elemental de Internet. A partir del concepto de *instrumentalidad*, y por medio de un análisis de dispositivo (*dispositif*), el artículo analiza Internet en su diseño fundamental y función estratégica, para mostrar la estrecha relación entre éste y la producción y administración de ignorancia como instrumento de una tercera persona. Se argumenta que la agnotología es un elemento sistémico de Internet que beneficia intereses y valores generalmente desconocidos.

PALABRAS CLAVE. Cambridge Analytica, medios digitales, diseño de Internet, libre flujo de la información, política exterior estadounidense.

POST-TRUTH, AGNOTOLOGY AND INSTRUMENTALITY ON THE INTERNET

ABSTRACT. In times of relativisation and discredit of truth, as mere opinion and manipulation (post-truth), and of deliberate use of the production and manipulation of ignorance (agnosto-

* Investigador independiente. Doctor en Política por la Universidad de Bristol, maestro en Comunicación y Política por la UAM-Xochimilco, México. Correo electrónico: rilm@protonmail.com

logy) increasingly mobilised through digital media, the relation between these practices and the core design of the Internet has not yet been addressed. Drawing on the concept of instrumentality and through a *dispositif* analysis, the article analyses the fundamental design of the Internet and its strategic function, to demonstrate the intertwinement between the latter and the production and management of ignorance as instrument of a third party. The main argument is that agnotology is a systemic component of the Internet that benefits generally unacknowledged values and interests.

KEY WORDS. Cambridge Analytica, digital media, Internet design, free flow of information, US foreign policy.

INTRODUCCIÓN

La época actual se ha caracterizado, principalmente a partir de experiencias anglosajonas y europeas, como una era o un régimen de posverdad (Pomarentsev, 2014; Prozorov, 2018; Tallis, 2016, Viner, 2016). En dicho régimen se habrían conjuntado algunas corrientes de extrema derecha, autoritarismos y desconfianza hacia los medios dominantes y hacia el conocimiento científico; todo en un contexto de expansión de nuevos medios y nuevas tecnologías de la información y dando como resultado la consolidación de una tendencia “antidemocrática” y “anti-progresista” (Prozorov, 2018; Tallis, 2016).

El objetivo de la práctica de posverdad, se afirma, es la creación de “inestabilidad o incluso la destrucción misma de la noción de Verdad (con V mayúscula)” (Tallis, 2016, p. 9. Traducción del autor). La figura en cuestión no dice la verdad (como correlación entre lo dicho y lo acontecido) sino utiliza mentiras evidentes y asociaciones engañosas para lograr sus objetivos personales y de grupo reducido (Tallis, 2016, p. 9). Tal régimen de posverdad estaría además apoyado en la informática y su “simplificación ilusoria de la realidad” (Curtis, 2016), como fue evidente en los casos de la primera campaña presidencial de Trump y la campaña para promover la salida de Reino Unido de la Unión Europea (Brexit).

Ambas campañas fueron desarrolladas por la firma de “comunicación estratégica” Cambridge Analytica, que utilizó información de al menos 87 millones de votantes, usuarios de la plataforma Facebook, y la analizó por medio de perfiles psicométricos personalizados y modelos de predicción del comportamiento de dichos usuarios para manipular sus preferencias y encausarlos, también por medio de anuncios y noticias falsas, a votar o actuar en favor de sus clientes (Grassegger y Krogerus, 2018). Aunque Trump y Brexit fueron los casos más conocidos, la compañía presumiblemente tuvo presencia en al menos otros 100 países entre los que se cuenta a México, afectando a casi un millón de usuarios en este país (BBC, 2018; Galdos, 2018).

El régimen de posverdad, apoyado en la vanguardia digital, en lugar de apelar al pensamiento comprometido, ha buscado explotar las emociones y la confianza, haciendo sentido de ellas y ofreciendo “interpretaciones atractivas y significativas sobre [la] condición actual y posibilidades futuras, a pesar de lo exageradas, fácticamente incorrectas o empíricamente sesgadas que puedan estar” (Tallis, 2016, p. 10. Traducción del autor). Por ello, la cultura de posverdad puede caracterizarse por una perspectiva relativista que “aproxima todas las verdades como si fueran meras opiniones o producto de intereses privados ocultos” (Prozorov, 2018, p. 18. Traducción del autor); aunque ella misma manipule la información, las emociones y la confianza de las personas de manera premeditada y velada. Los avances en informática, en conjunto con los modelos de predicción de conductas, parecen ser de los mejores aliados de esta práctica de manipulación (Curtis, 2016; Grassegger y Krogerus, 2018). Lo que cabe cuestionar es cómo entender esta alianza.

El régimen de posverdad, se presume, ha encontrado en los Estudios sobre Ciencia y Tecnología (ECT, Science and Technology Studies en inglés) a un muy apropiado expositor por reconocer el principio de “simetría” (Fuller, 2016)—según el cual todas las creencias, verdaderas o falsas, son consideradas en los mismos términos y tanto los seres humanos como los no-humanos tienen agencia y modelan los conocimientos y artefactos que se producen, al igual que dichos conocimientos y artefactos modelan las relaciones sociales y a los seres humanos y no-humanos (Law y Lin, 2017). Sin embargo, exponentes de los ECT

como Sergio Sismondo se han deslindado de ser fundamento o antecedente de tales prácticas al afirmar que “una democratización epistémica no significa el abaratamiento total del conocimiento tecnocientífico en el proceso” (2017, p. 3. Traducción del autor). El autor afirma que “los análisis detallados de los ECT sobre la construcción del conocimiento muestran que se requiere infraestructura, esfuerzo, ingenio y estructuras de validación”, lo que implica que el conocimiento puede “ser [siempre, aunque no fácilmente] de otra manera” pues siempre hay “otras infraestructuras, esfuerzos, ingenio y estructuras de validación posibles” (Sismondo, 2017, p. 3. Traducción del autor).

Centrándonos aquí en el estudio e importancia de los dispositivos tecnológicos en la expansión de una práctica de posverdad, cabe considerar, como señala Joanna Kempner que los ECT, además de investigar el contexto político, económico y social en que el conocimiento, la ciencia y la tecnología son producidas, cuestionan “la realidad de quién está siendo privilegiada y los intereses y necesidades de quién se están atendiendo”, quién está siendo excluido y quién es “sistemáticamente dañado por los desarrollos tecnológicos” y “cómo podemos resistir a estas relaciones de poder” (2020, p. 235. Traducción del autor).

Tal investigación puede ser realizada de manera diligente y sistemática para producir conocimiento confiable (Tallis, 2016, p. 9; Kempner, 2020, p. 235) sobre el papel de los medios digitales en un régimen de posverdad. Ello implica, de entrada en este caso, reinscribir el fenómeno de la “posverdad”, de reciente cuño (Shah, 2017), dentro del estudio de la producción y utilización intencional de la ignorancia o *agnostología* (Proctor, 2008), “un tema mucho más general que el de la cultura política de posverdad” (Hess, 2020, p. 242; Kempner, 2020, p. 235).

Ya que nula atención se ha prestado a la relación entre agnotología y diseño de Internet, el presente artículo busca responder a la pregunta: ¿cómo contribuye Internet, por su diseño mismo, a la producción, incluso intencional, de ignorancia? Ello con base en el concepto de *instrumentalidad* de Giorgio Agamben, el cual da cuenta de la mediación de una tercera persona y la producción de ignorancia que ello conlleva, y, metodológicamente, por medio de un análisis de “dispositivo” [*dispositif*] (Foucault, 1977). Así, se analiza Internet como un conjunto heterogéneo de elementos (incluyendo diseño, constitución, protocolo

central e instituciones sociales involucradas) para identificar su función estratégica, y la forma de coordinación que rige su operación, y detallar la estrecha relación entre diseño tecnológico y producción y manipulación de la ignorancia y de los usuarios como instrumentos de una tercera persona.

DE INSTRUMENTALIDAD E INTERNET: ¿QUIÉN CONTROLA QUÉ Y CÓMO?

Giorgio Agamben ha profundizado en la idea de instrumentalidad como rasgo característico de lo tecnológico, proponiendo que, desde cierta metafísica occidental, un instrumento es “un ser que, mientras vive [actúa] de acuerdo con su propio fin [y forma], es precisamente y por esa razón, y en la misma medida, usado para el fin de alguien más [el actor principal]” (2015, p. 75. Traducción del autor). Agamben agrega que “lo que parece definir a la causa instrumental es su indiferencia con respecto al fin que la causa principal [o actor principal] persigue”, “el instrumento ‘no sabe nada’ del producto final o la causa final pero es fundamental para ello” (2015, p. 73-74). Así, en esta noción de instrumentalidad, el instrumento, pese a ser fundamental para el logro del fin del actor principal, no sabe nada sobre dicho fin y es indiferente al mismo, mientras que el actor principal es más que un actor que se beneficia de la “naturaleza” y “autonomía” del instrumento. Como señala Agamben, “la tecnología es la dimensión que se abre cuando la operación del instrumento ha sido rendida como autónoma y al mismo tiempo es dividida en dos operaciones distintas y relacionadas” (2015, p. 74).

La primera operación refiere al instrumento como autónomo y la segunda es la que refiere al fin del actor principal, se trata de dos operaciones distintas pero relacionadas. Dicha forma “autónoma” del instrumento depende del fin que alguien más persigue, se inserta sin saberlo en una economía u orden que le define y le utiliza sin que él conozca dicho uso. El actor principal es quien ha definido la supuesta naturaleza y autonomía del instrumento con base en ciertos atributos que le son útiles dentro de cierta economía u orden que el mismo actor vuelve inmanente para el instrumento, pues al diseñar el instrumento y atribuirle un comportamiento natural con base en atributos selec-

cionados de acuerdo a sus fines, el actor principal define la autonomía del instrumento y la economía u orden que le rige sin que este mismo instrumento de cuenta de ello. Respecto a la tecnología moderna, el mismo autor señala que ella se caracteriza por un “potencial de obediencia” en el cual los aparatos

han incorporado en ellos mismos la operación del agente principal y pueden por tanto “obedecer” sus comandos (incluso si éstos están en realidad inscritos en el funcionamiento del aparato, de tal manera que aquél que los utiliza, al utilizar los “controles”, obedece en su lugar a un programa predeterminado) (Agamben, 2015, p. 77).

Desde esta perspectiva, Internet, que “(con I mayúscula) refiere a la red global específica de sistemas basados en el protocolo TCP/IP y que originalmente consistía en ARPAnet [Advanced Research Projects Agency network] y otras redes de investigación” (Hall, 2000, p. 5. Traducción del autor), implica una tercera persona como “más de un” agente y usuario en operación (Carr, 2015; Deibert y Crete-Nishihata, 2012; DeNardis y Hackl, 2015; Naughton, 2016; Powles, 2015), inscrito en el código y protocolo mismo que todo elemento del sistema debe obedecer (Galloway, 2004). Esta consideración difumina la distinción entre usuario final e instrumento, pues Internet oculta la operación y decisión de quienes definen la economía y los fines centrales del sistema, programando e incorporando valores e intereses en los aparatos que los usuarios comunes utilizan y por medio de los cuales “son utilizados”, pues su conducta y experiencia, como datos, devienen el objeto principal a explotar y dar forma (Couldry y Mejias, 2019).

Así, Internet integra una variedad de procesos y usuarios generalmente ignorados, como la infraestructura y la distribución de sus cables transoceánicos (Telegeography, 2019); “la nube” como enormes instalaciones de almacenamiento de datos y consumo de energía; o los algoritmos que procesan datos y los términos y condiciones de privacidad, que siempre implican la delegación del control sobre la “vida digital” propia a terceros que no conocemos (Hern, 2020).

La noción de “dispositivo” [*dispositif*], por su parte, implica un ensamble heterogéneo de elementos con una función estratégica y busca identificar “los elementos que participan en una racionalidad, una forma de co-ordinación dada” (Foucault, 1977, p. 197. Traducción del autor). A partir de ello, en continuidad con la noción de instrumentalidad, el análisis sigue las líneas estratégicas más generales, los intereses, los valores y las formas de conducir las interacciones entre los diferentes elementos de un mismo complejo. Ello, tras integrar las contribuciones de otras aproximaciones como la Construcción Social de la Tecnología (CST) (Bijker, 2010; Jassanof, 2004), la Teoría Crítica de la Tecnología (TCT) (Feenberg, 2002) y los Estudios sobre Ciencia y Tecnología en Relaciones Internacionales (ECT-RI) (McCarthy, 2015; Peoples, 2010) y reconocer la necesidad de analizar y comprender la función estratégica de los dispositivos a partir de la trayectoria histórica de su diseño tecnológico, pues ello resulta crucial para entender cómo y para quién actúan dichos dispositivos en su forma más general y sus implicaciones políticas.

Por lo anterior, dicho análisis identifica las formas de coordinación o racionalidades de gobierno que emergen cuando un conjunto de elementos (“discursivos” y “no discursivos”) es orientado hacia un objetivo específico (racionalidades siempre abiertas a reevaluación y reordenación estratégica) y produce objetos y sujetos en ese mismo entramado histórico y espacial (Foucault, 1977, 1997, Lemke, 2015). Así, Internet es analizado aquí en su historicidad, como un instrumento estructurado de forma particular de acuerdo a intereses particulares que no son entendidos sólo como intereses individuales sino también como “estrategias anónimas” (Foucault, 1977, p. 202) que sedimentan intereses en instituciones y valores, en procedimientos y lineamientos, en cuerpo y práctica, y que operan a pesar de tener o no autores individuales identificables a quienes las estrategias y el cálculo puedan ser atribuidas.

Con base en tal metodología, el presente análisis vincula política exterior, infraestructura, instituciones internacionales, valores e ideales, con procesos de producción de sujetos, prácticas diarias y ordenamientos de enunciación. Los resultados presentados a manera de narrativa retoman la historicidad de Internet, profundizan en la forma de coordinación con la que se ha organizado la red misma y con la que la red organiza sus

componentes, y enfatizan el predominio de E.U. como actor principal. El argumento central es que la forma de coordinación de Internet está directamente relacionada con la administración de ignorancia en beneficio de intereses y valores específicos generalmente desconocidos.

AGNOTOLOGÍA COMO COMPONENTE TÉCNICO Y SOCIAL DE INTERNET

Previo y durante los años en que Internet fue diseñado en su protocolo fundamental, sus diseñadores, que comprendían en su núcleo de toma de decisión al Departamento de Defensa, a la Agencia de Proyectos de Investigación Avanzada (ARPA en inglés) y a profesionales de universidades y laboratorios de Estados Unidos, dieron cuenta de la necesidad de administrar procesos de gran complejidad a partir de la simplificación del entorno social y técnico y por medio de prácticas y valores de fragmentación, funcionalización, flexibilidad y adaptabilidad de procesos (Abbate, 1999; Cerf y Kahn, 1974, 2006; Galloway, 2004; Hall, 2000; Lukasik, 2011; Naughton, 2000, 2016).

Para administrar y acomodar tanto la complejidad como la diversidad de los sistemas técnico y social, los diseñadores de ARPAnet e Internet emplearon estrategias de modularidad (*modularity*) y manejo por capas (*layering*), las cuales ocultaron tanto procedimientos básicos en diferentes niveles técnicos y sociales, como la economía general del sistema en un entorno político mundial beligerante (Abbate, 1999: 50; Galloway, 2004; McPherson, 2009). Así, Tara McPherson (2009) identifica la “modularidad” y el “manejo de la diversidad” como reglas y estrategias fundamentales para los sistemas operativos en computación y diseño de *hardware* desde los cincuenta, pero también, como respuesta a imperativos de seguridad propios de la Guerra Fría que permearon en áreas más amplias, como la cultural, racial, académica y política, en E.U. (e.g. la fragmentación de la producción académica y de luchas raciales y sindicales mundiales).

Acorde al estilo de administración informal y descentralizado de ARPA, que combinó eficiencia, jerarquía y control sutil de sistemas abiertos y elitistas de investigación (Hafner y Lyon, 1998, p. 17; Lukasik, 2011; McPherson, 2009), el manejo por capas (*layering*) y la modularidad (*modularity*) permitieron superar y acomodar la diversidad (técnica

y social) y ser capaces de construir y expandir la red (Abbate, 1999, p. 50). Esta estrategia limitó el conocimiento de la complejidad técnica del sistema para volverla manejable a través de la fragmentación en bloques modulares o capas con funciones y reglas de interacción específicas. Como Janet Abbate enfatiza, las implicaciones son tanto técnicas como sociales, pues “vuelve la complejidad técnica del sistema más manejable y permite al sistema ser diseñado y construido de manera descentralizada” (1999, p. 51. Traducción del autor). Mientras se utilicen las mismas interfaces, las capas “independientes” pueden ser “creadas y modificadas separadamente”; el diseñador sólo necesita saber “cómo se espera que la capa interactúe con otras capas” (Abbate, 1999, p. 51).

En última instancia, este principio de limitar y ocultar procesos técnicos complejos (y cruciales) permitiría al mercado computacional expandirse, ofreciendo interfaces “amigables al usuario” para incluir a los no familiarizados con la programación (Ceruzzi, 2003, p. 345; Hall, 2000, p. 6). Por ello, manejabilidad se traduce en ignorancia de los intrincados procesos implicados al desarrollar tareas independientes (instrumentales) y ajustarse, de manera velada o “descentralizada”, a la forma de interacción definida por terceras personas (economía general del sistema).

Igualmente, a nivel “social”, la organización del proyecto distribuyó las tareas entre grupos: la capa de comunicación la desarrolló la corporación privada Bolt, Beranek and Newman (BB&N), la Universidad de California en Los Ángeles y la Corporación de Análisis de Red (Network Analysis Corporation), mientras que los protocolos fueron asignados al Grupo de Trabajo de Red (Network Working Group) (Abbate, 1999; Cerf y Kahn, 1974, 2006). Así, el trabajo por capas ofreció a los diseñadores y usuarios una manera de ignorar procesos complejos y en operación mientras se utiliza el sistema. Cada componente parecía ser y funcionar por sí mismo, al desarrollar una tarea específica y tomar decisiones sólo en torno a dicha tarea; al igual que cada área científica, corporativa y administrativa era capaz de autorrepresentarse sus funciones, separando la investigación técnica de la función estratégica del conjunto; por ejemplo, de sus aplicaciones bélicas ligadas a la seguridad nacional durante la Guerra de Vietnam y ausentes en los reportes de investigación al Congreso (Abbate, 1999; Levine, 2018; Mosco, 1989).

Los miembros del sistema se volvieron entonces instrumentales: “no sabían nada” y eran intercambiables, lo que se consolidó en el protocolo central de Internet (véase Cerf y Kahn, 1974). El TCP/IP (Transmission Control Protocol/Internet Protocol) fragmenta y ordena los paquetes de datos y supervisa y controla su transferencia al seleccionar las rutas y encausar los paquetes para “mover los datos a través de la red” (Galloway, 2004, p. 42-44. Traducción de autor). Además, el TCP/IP “es una *familia* modular de protocolos” que contiene y provee de “un amplio rango de funciones segmentadas” (Hall, 2000, p. 6. Traducción del autor). “No es un protocolo monolítico único, sino una colección de protocolos que van desde funciones de aplicación específica como búsqueda web hasta protocolos de red de bajo nivel como IP y TCP”, por lo que funciona como un lenguaje y orientación común, omniabarcante, para elementos y funciones segmentadas (Hall, 2000, p. 6). Así, el control de la información está incorporado en un lenguaje compartido y su imaginación de autonomía: la red como compuesta de “sistemas inteligentes de extremo a extremo (end-point) que son auto-determinativos” (Hall, 2000, p. 6).

Internet como “la red global específica de sistemas basados en TCP/IP” (Hall, 2000, p. 5), instrumentaliza la auto-determinación de sus componentes dentro de una red expansiva y “sin costuras” (seamless) que, al segmentar y producir ignorancia, simplifica procesos mediante una creciente variedad de aplicaciones de uso general. Fragmentada y flexible pero siempre orientada, la forma de coordinación (Foucault, 1977) que es el protocolo se corresponde con la estrategia general de modularidad como función estratégica del *dispositif*. Esta última que administra y simplifica procesos al fragmentarlos en funciones autónomas y al acomodar su diversidad y limitar su conocimiento para manejar un sistema técnico y social complejo y expandirlo.

La modularidad, por tanto, es crucial, al fragmentar el conocimiento del todo en partes y funciones intercambiables para ocultar información acerca del funcionamiento general del sistema, sus jerarquías y capacidad de decisión. Esta forma de coordinación flexible y sutil implica cierto grado de descentralización (cada componente tiene una función pero ninguno es indispensable) y un balance específico entre autonomía y estabilidad general del sistema. Autónomamente, cada componente

desempeña su diseño como si fuese su naturaleza misma, sin saber nada sobre la finalidad principal y estratégica que sirve (instrumentalidad).

A través de la misma estrategia, el sistema ha hecho uso de cierta libertad, tanto en términos de sistemas de investigación abierta (o “blue sky” research), oportunidad comercial, interés individual y prestigio — que se puede interpretar como libertad empresarial y científica (Hafner y Lyon, 1998, p. 17), como de autonomía para las funciones de sus protocolos base (TCP/IP)— colección de protocolos y sistemas de punto final “inteligentes” (end-point systems) (Hall, 2000). Todo incorporando instrumentalmente un sentido de superioridad y seguridad nacional en competencia global, dependiente, hasta hoy día, del financiamiento y dirección del estado estadounidense (Mosco, 1989; Powers y Jablonski, 2014; SoD, 2014; TWH, 2018).

Internet ha estado orientado por la capacidad de sus diseñadores (estatales-corporativos) para establecer control en términos de superioridad, vanguardia tecnológica, compartición de recursos informáticos, comunicaciones seguras y ahorros financieros (como gastos de comunicación y uso de ordenadores), y por valores como competitividad económica, expansión de mercado y aplicaciones civiles y militares que rindan ventajas nacionales (Abbate, 1999; DARPA, 2018; Edwards, 1996; Lukasik, 2011; Mazzucato, 2014). Internet entrelaza, instrumentalmente, imperativos de control con la flexibilidad y las ventajas de la autonomía, velando además sus prerrogativas gubernamentales.

El estado estadounidense, por medio de agencias de gobierno como DARPA y la CIA, ha sido crucial para las industrias en Silicon Valley, financiando y fomentando, dentro de los márgenes de la seguridad nacional, la investigación y el desarrollo tanto con aplicación en tareas de inteligencia y milicia, como con aplicación comercial que apuntale la presencia corporativa de E.U. en el mundo (e.g. “el estado detrás del iPhone” [Mazzucato, 2014]; Keyhole, un software de mapeo adquirido por Google y fundamento de Google Maps y Google Earth; o el *Systems Research Development*, una herramienta de mineo de datos para uso judicial y policiaco, ahora propiedad de IBM [Blank, 2011; Henn, 2012; Powers y Jablonski, 2015, p. 66-67]). Además, la explotación masiva de datos —Big Data (Mayer-Schönberger y Cukier, 2013)— ha conjuntado a agencias gubernamentales, corporaciones privadas y

contratistas de seguridad (Cohen, 2010; Fuchs, 2017; Vanian, 2015) para combinar gozo, participación y comercio (bajo la apariencia de libertad) con vigilancia y control (bajo el imperativo de seguridad comercial y militar) (Zuboff, 2019) y consolidar a Internet dentro de la planeación estratégica estatal estadounidense (Hansen y Nissenbaum, 2014; Reveron, 2012; EOPUS, 2009; TWH, 2018).

Internet, como *dispositivo*, implica entonces una orientación estratégica general y un orden espacial acorde a la seguridad nacional como beneficio comercial y expansión global (EOPUS, 2009; SoD, 2014; TWH, 2018). Su protocolo y estrategias de modularidad han sido su forma de gobernar elementos heterogéneos como un sistema flexible y distribuido. Su economía visibiliza libertad e innovación, persuade, mientras simplifica y maneja un entorno técnico y social complejo a nombre de sus usuarios y produce y administra su ignorancia en aras de imperativos anónimos. De esta manera, el diseño mismo de Internet ha producido y administra la ignorancia de sus usuarios, indiferentes e incapaces de discernir las diferentes capas de procesos y la mediación que crecientemente hacen posible su nuevo entorno e interacciones. Con ello, se oculta la economía y los intereses que guían la operación general de dicha tecnología y las implicaciones políticas de ello, pues tal ignorancia es elemental para el funcionamiento del sistema. Acorde a este diseño, el siguiente apartado destaca cómo se entreveran agnología y expansión de Internet mediante el “libre” flujo de información como imperativo estadounidense en política mundial.

LIBERTAD DE INTERNET Y EL LIBRE FLUJO DE LA INFORMACIÓN: MEDIACIÓN Y FRAGMENTACIÓN DEL CONOCIMIENTO Y LA ORIENTACIÓN COLECTIVA

Naciones Unidas consideró la libertad de Internet un derecho humano en 2011 y lo reafirmó en 2016, al condenar la interrupción intencional del acceso a la red (HRC, 2016). Sin embargo, ésta ya era, hace tiempo, ampliamente promovida por el gobierno estadounidense junto con el libre flujo de la información y otros derechos humanos acordes a su agenda particular. Así, la Estrategia Internacional para el Ciberespacio (EOPUS, 2011) señala que un ciberespacio abierto e interoperable, seguro y confiable, y estable normativamente, es imperativo, pues

Estados Unidos está comprometido con iniciativas y estándares internacionales que fortalecen la ciberseguridad mientras salvaguarda el libre comercio y el más amplio libre flujo de la información, reconociendo nuestras responsabilidades globales, así como nuestras necesidades nacionales.

El imperio de la ley, un orden civil en el cual la fidelidad a las leyes salvaguarda a las personas y a los intereses, brinda estabilidad a los mercados globales y sujeta a actores malevolentes a responder internacionalmente, apoya tanto a nuestra seguridad nacional como al avance de nuestros valores comunes (EOPUS, 2011, p. 5. Traducción del autor).

Acorde a ello, el papel de E.U. respecto al ciberespacio implica diplomacia, seguridad y “libre comercio”, para en última instancia lograr la expansión de mercados, la aplicación de la ley y la defensa bajo parámetros estadounidenses. La promoción del libre flujo de la información figura así como parte de una estrategia de liberalización basada en la apertura de mercados foráneos y la expansión de democracias liberales (Carr, 2013; Powers y Jablonski, 2015, p. 37; McCarthy, 2015). Dicha tarea, en Estados Unidos, “ha informado la estrategia y las políticas internacionales de comunicaciones en sus aspectos político y económico” (McCarthy, 2015, p. 74) desde las primeras décadas del siglo veinte. La expansión de Internet, bajo tal premisa, colabora a extender el capitalismo como orden económico y cultural y lograr el orden internacional que E.U. avizora a través de su política exterior (Foley, 2007).

Complementando tal programa de política exterior, se encuentran los “programas diplomáticos que fueron diseñados para persuadir, informar, y atraer la opinión pública global al servicio de los intereses nacionales [estadounidenses]” (Graham, 2015, p. 1. Traducción del autor). Tales esfuerzos han producido y utilizado normas culturales y valores para avanzar sus propios objetivos. Tal es el caso de la administración Obama y la promoción del uso de Internet para la movilización social en otros países (USDoS, October 2009). Por ejemplo, el fomento de Hillary Clinton a la difusión de tecnologías para evadir la vigilancia estatal (*circumvention technologies*) en otros países (como los de la denominada “Primavera Árabe”) y el patrocinio, junto con *Google*, *Facebook*

y otras empresas, de los Encuentros de la Alianza de Movimientos de la Juventud (*Alliance of Youth Movements summits*) hablan de cómo E.U. ha usado Internet para avanzar sus intereses en política exterior, incluso manipulando pancartas de movimientos sociales (Aouragh y Chakravarty, 2016; Carr, 2013; Mejias, 2010).

Mientras en los años 80 las personas eran alfabetizadas en versiones “amigables al usuario” y para el 2001 ya eran objeto de explotación, para el 2009, el marco normativo de la libertad de Internet aparece como “expresión del poder estructural e institucional de E.U.” (Carr, 2013, p. 622) e ideología central de su política exterior, particularmente clara desde que Clinton era Secretaria de Estado y no menos importante para el gobierno de Trump (TWH, 2018).

Junto al plano ideológico y normativo de la libertad de Internet, el modelo de gobernanza global de múltiples participantes de Internet (*multi-stakeholder*), que reúne al sector privado, al sector público y a la sociedad civil, ha sido un refuerzo del actual status quo en política internacional. Este modelo ha beneficiado a los actores involucrados en el diseño y desarrollo de esta tecnología; particularmente, a aquellos del sector privado estadounidense que el gobierno de Bill Clinton apoyó (Carr, 2015). Se trata de un modelo dominado por los intereses de E.U. (Powles, 2015), en el cual la sociedad civil figura como un actor de legitimación bajo el predominio de multinacionales estadounidenses y de gobiernos aliados (Carr, 2015, p. 642). Más aún, se trata de un modelo que implica una forma de administrar la participación a nivel mundial por medio de élites especializadas, coordinando diferentes actores transnacionales y nacionales y promoviendo el “excepcionalísimo de Internet” por medio de la exclusión de “perspectivas [y partidarios] a favor de la soberanía y la anti-mercantilización de la gobernanza de Internet... de los debates” (Chenou, 2014, p. 206. Traducción del autor).

Pese a lo anterior, incluso activistas de izquierda y progresistas promueven el excepcionalísimo de Internet al ignorar que responde en gran medida a ideales y valores de derecha y al enfatizar el potencial de participación de la sociedad civil (Golumbia, 2015, p. 15). Así, un modelo específico de gobernanza, que beneficia la mercantilización de datos y de usuarios, ha sido apoyado por diversidad de ideologías con base en el desconocimiento y la imaginación común de Internet

como excepcional y apolítica, “neutral” y abierta a un uso instrumental (Golumbia, 2015, p. 15). Lo que no implica que ningún gobierno deba regular Internet sino que el control gubernamental ha de tomar una forma cercana a la administración informal o flexible del gobierno estadounidense. La gobernanza de Internet impulsa una práctica particular de gobierno, la estadounidense, basada en un balance específico entre componentes militares, corporativos y civiles y en fundamentos capitalistas como el presupuesto de que los datos son una mercancía.

El libre flujo de la información e Internet libre complementan así “una tendencia a usar las leyes de telecomunicaciones y las exportaciones relacionadas con tecnologías de la información para promover los intereses económico políticos de E.U. alrededor del mundo”, en la cual “la idea de la información como algo apolítico, culturalmente neutral, y capaz de ser comprado y vendido como parte de un intercambio global de bienes y servicios” (Powers y Jablonski, 2015, p. 22) ha sido fundamental para un mayor acceso y explotación de datos de acuerdo con agendas desconocidas (Grasseger y Krogerus, 2017; Zuboff, 2019).

En casos como el de China, pese a su orientación nacional y gran competencia a nivel de infraestructura, protocolos y aplicaciones, muchas de las formas y valores tecnológicos occidentales, como la información como mercancía, siguen vigentes. Ello implica cierta continuidad en el condicionamiento de la soberanía de los estados y consolida a la información como activo explotable bajo el abrigo de una ley de comercio internacional que beneficia un mercado mundial de actores establecidos (Powers y Jablonski, 2015, p. 10; Reid, 2009, p. 609).

Asimismo, la prioridad que se ha otorgado al Artículo 19 de la Declaración Universal de Derechos Humanos, sobre libertad de expresión, por encima del Artículo 29, sobre la autodeterminación de los pueblos, ha sido promovida por la política exterior estadounidense para Internet y se apoya en y promueve la mercantilización de los datos. Como señala McCarthy, “la importancia de la libertad de discurso y expresión como un derecho humano universal es constantemente expresado a lo largo del discurso estadounidense” y su consolidación se remonta “al final de la primera fase del Encuentro Mundial sobre la Sociedad de la Información”, lo que ha significado un alto costo económico y político para China y otros países (2015, p. 103).

En esta línea, valores económicos liberales (en política exterior) y capitalistas constituyen la condición básica para la soberanía, ya que “quienes elaboran las políticas públicas en E.U. simultáneamente trabajan para socavar la legitimidad del derecho a la autodeterminación de otros estados” (McCarthy, 2015, p. 104), lo que condiciona otras concepciones de soberanía dependiendo del grado en que se sujeten a valores culturales occidentales (Carr, 2013; Powers y Jablonski, 2015; McCarthy, 2015) y no contravengan los intereses de actores dominantes. El libre flujo de la información asume e impone que el acceso no debe ser negado o restringido sobre bases ideológicas o políticas distintas a las occidentales (McCarthy, 2015, p. 111-121), mientras oculta sus propios intereses, valores y procesos materiales, y fabrica y explota interacciones y conductas como datos.

Aunado a lo anterior, como una forma de coordinar cosas (Foucault, 1977; Lemke, 2015) y de producir ignorancia (Proctor, 2008), más allá de las leyes, las exportaciones y la retórica sobre la libertad, con el “libre flujo de la información” es la forma de Internet y “las normas y reglas físicas, materiales, [las que también] limitan la manera en que la tecnología puede ser usada, y por tanto las prácticas que uno puede llevar a cabo” con ella (McCarthy, 2015, p. 67). Los valores incorporados en la arquitectura material y programática, el *hardware* y el *software*, o los niveles de infraestructura, protocolos y aplicaciones de Internet, “reflejan el contexto de su creación, transparentando un sesgo liberal [económico] expresado de mejor manera en la noción de ‘libre flujo de la información’” (McCarthy, 2015, p. 9). Lo que significa que al “incluir o excluir ciertas prácticas... [una tecnología] previene y promueve objetivos en línea con aquellos de sus diseñadores”, lo que con Internet se hace visible tanto en una arquitectura de “end-point systems”—o de “extremo a extremo”, en la cual los contenidos de una comunicación no son discriminados durante su flujo—como en la gobernanza específica que vuelve costosa toda regulación gubernamental distinta a la definida por E.U. y sus aliados (McCarthy, 2015, p. 9).

Tales discriminaciones implícitas del libre flujo de la información se basan en valores culturales y preocupaciones de seguridad occidentales, y por tanto, en discriminaciones culturales más sutiles que tienen un amplio impacto sobre cómo los individuos son producidos como

sujetos. Así, en términos de lo que Jodi Dean llama “capitalismo comunicativo”, tal sesgo oculto de la “libertad” refiere a una “formación económico-política” que profundiza el declive de la “eficacia simbólica”, una ruptura en la significación colectiva, la fragmentación del reconocimiento del “peso simbólico del otro” en medio del “abrumador” flujo de contenidos (o el declive de una verdad compartida y significativa colectivamente), y la proliferación de incertidumbre en lo que refiere a política (Dean, 2009, p. 162).

El “otro”, ya sea un individuo o un colectivo hablando desde otro conocimiento o praxis, es desde el inicio distante, componente de una tecnología presuntamente neutral y reducido a datos ahora administrados y vendidos como mercancía. Sin ser considerados como sujetos, los usuarios son instrumentos, “no saben nada” de los procesos y la economía general que les maneja y opera a partir de ellos mismos, en una lógica de ganancia y seguridad nacional que define a las más populares y exitosas plataformas de Internet. Como Christian Fuchs señala respecto a Facebook, “[la plataforma] es el epítome del capitalismo digital: trata los datos personales como una mercancía para vender anuncios dirigidos [que] son conducidos por algoritmos que son ciegos [o selectivos] sobre el contenido de lo que se está anunciando”, por lo que afirma, “no es sorpresa que Facebook ha tolerado prácticas de manejo de datos sumamente problemáticas. Su lógica es que entre más actividad en línea, datos y metadatos se generen, mayores ganancias potenciales” (Fuchs, 2018).

Así, el capitalismo digital ha sido, a pesar de su supuesta neutralidad, ideológicamente selectivo y flexible, buscando también conducir las conductas de sus usuarios de manera velada (DeNardis y Hackl, 2015; Kramer *et al.*, 2014; Zuboff, 2019). Las plataformas digitales han sido capaces de reducir la verdad y la ideología a ideas y datos, útiles cuando son desarrolladas sin perturbar la generación de ganancias económicas y la seguridad nacional. Esta manera de operar pasa fácilmente desapercibida, pues vuelve flexibles y adaptables, al interior de su economía capitalista, a otros conocimientos (incluso subversivos) a través del sutil desvanecimiento de su significado y orientación colectivas. En el ambiente de Internet, las ideas pueden florecer en heterogeneidad siempre y cuando no perturben los valores occidentales generalmente

observados o lo hagan en favor de la generalizada y expansiva acumulación de capital y el modelo de seguridad nacional que le procura. Todo lo que pueda ser transformado en una mercancía puede ser tolerado, ofreciendo cierto sentido de neutralidad ideológica y cultural bajo la ilusión del libre flujo de la información y los usos alternativos de Internet, pero ocultando valores y capacidades de decisión y control.

Una vez presupuesto que la información y la expresión fluyen libres y que los gobiernos no deben regular Internet, se oculta su sesgo cultural y discriminaciones de contenido, inhibiendo el conocimiento y delegando la administración de la información, las comunicaciones e incluso las conductas a una tercera persona. Al manejar de manera velada la realidad social en versiones simplificadas, la posibilidad de producir conocimiento compartido y una verdad colectivamente significativa es obliterada por la cantidad y segregación de la información y las limitaciones sociales de esta tecnología por su diseño mismo.

Al ser capaz de acomodar la heterogeneidad a través de la flexibilidad, haciendo uso de visiones alternativas, opiniones y prácticas de organización social y economía e incrementando las variedades de contenido generado por los usuarios y el intercambio comunicativo, la habilidad de Internet para producir conocimiento y orientación política compartida (más allá de la alfabetización digital básica, la mercantilización y la propiedad privada) está limitada por su diseño mismo. Múltiples verdades instrumentales y significados fragmentados, o las llamadas “islas de información” (Berners-Lee, 2010), dificultan una ética compartida en una economía que en general se oculta y se vuelve implícita. Como consecuencia, la instrumentalidad abre la posibilidad de una práctica expansiva de *agnetología* (Proctor, 2008), como la producción intencional de ignorancia y ambigüedad, o quizás, más recientemente, de “posverdad”, “noticias falsas” y manipulación, como en los casos de Cambridge Analytica o del SARS-Cov-2 y en continuidad con un proceso de mediación velada que se remonta al diseño elemental de Internet.

CONCLUSIÓN

El presente artículo buscó comprender de qué manera contribuye el diseño mismo de Internet a la producción y manipulación, incluso

intencional, de la ignorancia de sus usuarios. A partir de la noción de instrumentalidad, se enfatizó la presencia de E.U. como tercera persona y de su estrategia anónima de producción de ignorancia al incorporar sus intereses y economía en los artefactos tecnológicos y en los usuarios comunes de los mismos. Por medio de un análisis de dispositivo [*dispositif*] y al explorar el diseño de la red, de su protocolo central, y de las instituciones sociales involucradas, se identificó la forma de coordinación de sus elementos constitutivos como una forma de administración informal que busca simplificar procesos a partir de la fragmentación del conocimiento general y compartido sobre la economía y función estratégica de esta tecnología. Dicha fragmentación implica la producción instrumental de ignorancia como elemento sistémico para la simplificación y manejabilidad de su complejidad técnica y social. Por su diseño técnico y social, Internet oculta sus puntos y lógicas de control mientras enfatiza sus atributos de autonomía, flexibilidad y apertura.

El estudio también identificó la función estratégica de Internet en el ámbito de la política mundial y nacional estadounidense, en apego a valores distintivos de esta nación (propiedad privada, empresariedad, autonomía, flexibilidad, adaptabilidad) y su agenda de política exterior en busca de la apertura de mercados y la expansión en la explotación de recursos. Se mostró cómo el diseño mismo de Internet hace posible y requiere de la ignorancia de sus usuarios, del que sean indiferentes e incapaces de discernir las múltiples capas de procesos y la mediación que hacen posible su nuevo entorno e interacciones.

El precio de tal simplificación y eficiencia es la fragmentación del conocimiento compartido sobre cómo opera y cuáles son sus implicaciones políticas, pues se desconoce quiénes—como individuos, grupos y estrategias anónimas—se benefician en última instancia de tal mediación. El usuario común delega así la capacidad de comprender y de manejar por sí mismo su entorno social y tecnológico, apuntalando la imagen de “neutralidad” de estas tecnologías y su ignorancia asociada. Así, no es de sorprender que la explotación y manipulación de la información, las conductas y la ignorancia, sean cada vez más invasivas y eficaces, como en el caso de Facebook o Google, pues el diseño de los soportes tecnológicos promueve la ignorancia que se transforma en resignación, comodidad o confianza en la “neutralidad” de los mismos.

Acorde al diseño técnico y social de la red, un “Internet libre” y el “libre flujo de la información”, sin una encarnación política y un conocimiento compartido de su economía y valores incorporados, benefician el proceso de mediación que fragmenta y mercantiliza el conocimiento, la interacción y la experiencia social. Dicha mediación, además de manejar procesos complejos por los usuarios, difunden formas capitalistas, estadounidenses y occidentales mediante un grupo reducido de especialistas y dentro de un modelo económico específico.

Ninguna tecnología es políticamente neutral y para poder utilizarla en beneficio de una sociedad, se debe comprender en toda su complejidad política, social, económica, cultural e incluso filosófica. Si se decide utilizar estas tecnologías, se debe ser capaz de comprender y reinscribir las pautas y valores incorporados en ellas, desde sus cableados y protocolos hasta sus aplicaciones más específicas; se ha de tomar parte de su constante diseño y expansión en cada una de sus facetas y estar al tanto de los riesgos que implica el no poder redefinir del todo algo que fue diseñado por un tercer actor, cuyos valores e intereses, a manera de sesgo, predominan. Con base en ello, se podrán tomar mejores decisiones en cuanto al alcance de estas tecnologías y sobre todo, a las instituciones sociales y políticas que son necesarias para comprenderlas y relacionarse con ellas, sin socavar el conocimiento y prácticas compartidas de una comunidad política.

FUENTES CONSULTADAS

- ABBATE, J. (1999). *Inventing the Internet*. Londres: The MIT Press.
- AGAMBEN, G. (2015). *The Use of Bodies, Homo Sacer IV*, 2. California: Stanford University Press.
- AOURAGH, M. y CHAKRAVARTY, P. (2016). Infrastructures of Empire: Towards a Critical Geopolitics of Media and Information Studies. En *Media, Culture & Society*. Vol. 38. Núm. 4. pp. 559-575. DOI: <https://doi.org/10.1177/0163443716643007>
- BBC (2018). Cambridge Analytica: the Data Firm's Global Influence. En BBC. Recuperado de: <https://www.bbc.com/news/world-43476762>

- BERNERS-LEE, T. (2010). Long Live the Web: a Call for Continuous Open Standards and Neutrality. En *Scientific American*. Recuperado de: <<http://www.scientificamerican.com/article.cfm?id=long-live-the-web>> Consultado el 29 de septiembre de 2013.
- BIJKER, W. (2010). How is technology made? – That is the question! En *Cambridge Journal of Economics*. Núm. 34. pp. 63-76. DOI: <https://doi.org/10.1093/cje/bep068>
- BLANK, S. (2011). *The Secret History of Silicon Valley*. University of California Berkeley. Recuperado de: <https://www.sam-network.org/video/the-secret-history-of-silicon-valley#!>
- CARR, M. (2015). Power Plays in Global Internet Governance. En *Millennium: Journal of International Studies*. Vol. 43. Núm. 2. pp. 640-659.
- CARR, M. (2013). Internet freedom, human rights and power. En *Australian Journal of International Affairs*. Vol. 67. Núm. 5. pp. 621-637. DOI: <https://doi.org/10.1080/10357718.2013.817525>
- CERF, V. y KAHN, R. (2006). *Oral History of Robert Kahn*. Virginia: Computer History Museum.
- CERF, V. y KAHN, R. (1974). A Protocol for Packet Network Intercommunication. En *IEEE Transactions on Communications*. Vol. COM-22. Núm. 5. pp. 637-648. Recuperado de: <<https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf>>
- CERUZZI, P. (2003). *A History of Modern Computing*. Cambridge y Londres: The MIT Press.
- CHENOU, J. (2014). From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s. En *Globalizations*. Vol. 11. Núm. 2. pp. 205-223. DOI: <https://doi.org/10.1080/14747731.2014.887387>
- COHEN, E. (2010). *Mass Surveillance and State Control*. Nueva York: Palgrave.
- COULDRY, N. y MEJIAS, U. (2019). *The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism*. California: Stanford UP.

- CURTIS, A. (productor). (2016). *Hypernormalisation*. Documental, BBC film.
- DARPA (2018). *DARPA: Defense Advanced Research Projects Agency 1958-2018*. Florida: Faircount Media Group.
- DEAN, J. (2009). *Democracy and Other Neoliberal Fantasies: Communicative Capitalism and Left Politics*. USA: Duke University Press.
- DE NARDIS, L. y HACKL, A. (2015). Internet Governance by Social Media Platforms. En *Telecommunications Policy*. Vol. 39. Núm. 9. pp. 761-770. DOI: <https://doi.org/10.1016/j.telpol.2015.04.003>
- DEIBERT, R. y CRETE-NISHIHATA, M. (2012). Global Governance and the Spread of Cyberspace Controls. En *Global Governance*. Núm. 18. pp. 339-361.
- EDWARDS, P. (1996). *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge: The MIT Press.
- EXECUTIVE OFFICE OF THE PRESIDENT OF THE U.S. (EOPUS). (2009). *Cyberspace Policy Review (CPR)*, Department of Homeland Security. Recuperado de: https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- EXECUTIVE OFFICE OF THE PRESIDENT OF THE U.S. (EOPUS) (2011) *International Strategy for Cyberspace*. The White House. Recuperado de: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspac_e.pdf
- FEENBERG, A. (2002). *Transforming Technology: A Critical Theory Revisited*. Oxford: Oxford University Press.
- FOLEY, M. (2007). *American Credo: The Place of Ideas in US Politics*. Oxford: Oxford University Press.
- FOUCAULT, M. (1977). Confessions of the flesh. En Gordon, C. (ed.). *Power/Knowledge: Selected Interviews and Other Writings 1972-197*. pp. 194-228. Nueva York: Pantheon Books.
- FOUCAULT, M. (1997) Technologies of the self. En Rabinow, P. (ed.). *The Essential Works of Michel Foucault 1954-1984, Volume 1: Ethics, Subjectivity and Truth*. Nueva York: The New York Press.
- FULLER, S. (2016). Embrace the Inner Fox: Post-Truth as the STS Symmetry Principle Universalized. En *Social Epistemology Review and Reply Collective*. Núm. 25. Diciembre, Recuperado de: <https://social-epistemology.com/2016/12/25/embrace-the-in->

- ner-fox-post-truth-as-the-sts-symmetry-principle-universalized-steve-fuller/
- FUCHS, Ch. (2017). *Social Media: A critical introduction*. Londres: Sage.
- FUCHS, Ch. (2018). What would Marx have said about Facebook and Cambridge Analytica? En *Open Democracy*. Recuperado de: <https://www.opendemocracy.net/uk/christian-fuchs/what-would-marx-have-said-about-facebook-cambridge-analytica>
- GALDOS, G. (2018). Cambridge Analytica: The Mexico allegations. En *Channel 4*. Recuperado de: <https://www.channel4.com/news/cambridge-analytica-the-mexico-allegations>
- GALLOWAY, A. (2004). *Protocol: How control exists after decentralization*. Cambridge: The MIT Press.
- GOLUMBIA, D. (2015). *The Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis: University of Minnesota Press.
- GRAHAM, S. (2015). *Culture and Propaganda: The Progressive Origins of American Public Diplomacy, 1936–1953*. Surrey: Ashgate.
- GRASSEGGER, H. y KROGERUS, M. (2018). The Data That Turned the World Upside Down. How Cambridge Analytica used your Facebook data to help the Donald Trump campaign in the 2016 election. En *Motherboard*. Recuperado de: https://www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win
- HAFNER, K. y LYON, M. (1998) *Where Wizards stay up late: The origins of the Internet*. Nueva York: Touchstone.
- HALL, E. (2000). *Internet Core Protocols: The Definitive Guide*. US: O'Reilly.
- HANSEN, L. y NISSENBAUM, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. En *International Studies Quarterly*. Núm. 53. pp. 1155-1175. DOI: <https://doi.org/10.1111/j.1468-2478.2009.00572.x>
- HENN, S. (2012). In-Q-Tel: The CIA's Tax-Funded Player In Silicon Valley. En *NPR: All Tech Considered*. Recuperado de: <http://www.npr.org/sections/alltechconsidered/2012/07/16/156839153/in-q-tel-the-cias-tax-funded-player-in-silicon-valley>
- HERN, A. (2020). Internet Privacy: the Apps That Protect you from four apps. En *The Guardian*. Recuperado de: <https://www.theguardian.com/technology/2020/feb/16/internet-privacy-settings-apps-to-protect-you->

- Hess, D. (2020). The Sociology of Ignorance and Post-Truth Politics. En *Sociological Forum*. Vol. 35. Núm. 1. pp. 241-249. DOI: <https://doi.org/10.1111/socf.12577>
- HUMAN RIGHTS COUNCIL (HRC). (2016). Oral Revisions of 30 June: Promotion and Protection of all Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development. En *United Nations*. 27 Junio.
- JASSANOF, S. (2004). The idiom of co-production y Ordering knowledge, ordering society. En Jassanof, S. (ed.) *States of Knowledge: The co-production of science and social order*. pp. 1-45. Londres: Routledge.
- KEMPNER, J. (2020). Post-Truth and the Production of Ignorance. En *Sociological Forum*. Vol. 35. Núm. 1. pp. 234-240. DOI: <https://doi.org/10.1111/socf.12576>
- KRAMER, A., GUILLORY, J. y HANCOCK J. (2014). Experimental Evidence of Massive-scale Emotional Contagion Through Social Networks. En *Proceedings of the National Academy of Sciences of the United States of America*. Vol. 111. Núm. 24. pp. 8788-8790. DOI: <https://doi.org/10.1073/pnas.1320040111>
- LAW, J. y WEN-YUAN, L. (2017). Provincializing STS: Postcoloniality, Symmetry, and Method. En *East Asian Science, Technology and Society: An International Journal*. Núm. 11. pp. 211-227. DOI: <https://doi.org/10.1215/18752160-3823859>
- LEMKE, Th. (2015). New Materialisms: Foucault and the 'Government of Things'. En *Theory, Culture & Society*. Vol. 32. Núm. 4. pp. 3-25. DOI: <https://doi.org/10.1177/0263276413519340>
- LEVINE, Y. (2018). *Surveillance Valley: The Secret Military History of the Internet*. Nueva York: Public Affairs.
- LUKASIK, S. (2011). Why the Arpanet Was Built. En *IEEE Annals of the History of Computing*. Vol. 33. Núm. 3. pp. 4-20. DOI: <https://doi.org/10.1109/MAHC.2010.11>
- MÄYER-SCHÖNBERGER, V. y CUKIER, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Houghton Mifflin Harcourt.
- MAZZUCATO, M. (2014). *The Entrepreneurial State: Debunking Public vs Private sector myths*. Londres: Anthe Press.

- MCCARTHY, D. (2015). *Power, Information Technology, and International Relations Theory: The power and politics of US foreign policy and the Internet*. Londres: Palgrave Macmillan.
- MCPHERSON, T. (2009). Why Are the Digital Humanities So White? or Thinking the Histories of Race and Computation. En *Debates in the Digital Humanities*. pp. 139-160. Minneapolis: University of Minnesota Press. DOI: 10.5749/minnesota/9780816677948.003.0017
- MEJIAS, U. (2010). *Off the Network: Disrupting the Digital World*. Minneapolis y Londres: University of Minnesota Press.
- MOSCO, V. (1989). *The Pay-per Society: Computers and Communication in the Information Age: Essays in Critical Theory and Public Policy*. Norwood: Ablex.
- NAUGHTON, J. (2000). *A Brief History of the Future: The origins of the Internet*. Londres: Phoenix Books.
- NAUGHTON, J. (2016). The evolution of the Internet: from Military Experiment to General Purpose Technology. En *Journal of Cyber Policy*. Vol. 1. Núm. 1. pp. 5-28.
- PEOPLES, C. (2010). *Justifying Ballistic Missile Defense: Technology, Security and Culture*. Nueva York: Cambridge University Press.
- POWERS, S. y JABLONSKI, M. (2015). *The Real Cyber War: the Political Economy of Internet Freedom*. Chicago: University of Illinois Press.
- PROCTOR R. N. (2008). Agnotology: a Missing Term to Describe the Cultural Production of Ignorance (and its study). En Proctor R. N. and Schiebinger L. (Eds). *Agnotology: The Making and Unmaking of Ignorance*. pp. 1-33. Stanford: Stanford University Press.
- PROZOROV, S. (2019). Why is there truth? Foucault in the age of post-truth politics. En *Constellations*. Núm. 26. pp. 18-30. DOI: <https://doi.org/10.1111/1467-8675.12396>
- POMARENTSEV, P. (2014). *Nothing is True and Everything is Possible*. Londres: Public Affairs.
- POWLES, J. (2015). Can the Internet be Saved Without Harming Democracy? En *The Guardian*. Recuperado de: <http://www.theguardian.com/technology/2015/apr/17/can-the-Internet-be-saved-without-harming-democracy>

- REID, J. (2009). Politicizing Connectivity: Beyond the Biopolitics of Information Technology in International Relations. En *Cambridge Review of International Affairs*. Núm. 22. pp. 607-623. DOI: <https://doi.org/10.1080/09557570903325520>
- REVERON, D. (2012). An Introduction to National Security and Cyberspace. En Reveron, D. (Ed.). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. pp. 3-20. Washington, DC: Georgetown University Press.
- SECRETARY OF DEFENSE (SoD). (2014). *Quadrennial Defense Review (QDR)*. Washington, DC: Defense Pentagon, Recuperado de: http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf
- SHAH, H. (2017). Post-truth publications. En *Significance*. Vol. 14. Núm. 5. p. 45.
- SISMONDO, S. (2017). Post-Truth?. En *Social Studies of Science*. Vol. 47. Núm. 1. pp. 3-6. DOI: <https://doi.org/10.1177/0306312717692076>.
- TALLIS, B. (2016). Living in Post-truth: Power, Knowledge/Responsibility. En *New Perspectives*. Vol. 24. Núm. 1. pp. 7-18.
- TELEGEOGRAPHY (2019). Submarine Cable Map 2019. En *Telegeography Maps*. Recuperado de: <https://submarine-cable-map-2019.telegeography.com/>
- THE WHITE HOUSE (TWH). (2018). *National Cyber Strategy of the United States of America*. Recuperado de: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
- US DEPARTMENT OF STATE (USDoS) (October 2009). *Alliance of Youth Movements Summit*, Office of the Spokesman, Octubre 13, Washington, DC. Recuperado de: <https://2009-2017.state.gov/r/pa/prs/ps/2009/oct/130503.htm>
- VANIAN, J. (2015). What the CIA and Silicon Valley have in Common. En *Fortune tech*. Recuperado de: <http://fortune.com/2015/06/16/cia-silicon-valley-common/>
- VINER, K. (2016). The Long Read: How technology disrupted the truth. En *The Guardian*. Recuperado de: <https://www.theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth>

ZUBOFF, S. (2019). *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*. Londres: Profile Books.

Fecha de recepción: 31 de enero de 2021

Fecha de aceptación: 20 de abril de 2021

DOI: <http://dx.doi.org/10.29092/uacm.v18i46.841>