

Una aproximación Hayekiana a las amenazas en contra de la libertad individual en las redes sociales de Occidente

Chantal Soldini

Resumen

El propósito de este ensayo es explorar el estado de la libertad individual en redes sociales, en particular su infraestructura y consecuencias sociales. Este ensayo también elaborará por qué es de interés un análisis de libertad en las redes sociales, el rol de *Big Data* en el capitalismo informático y la posibilidad de una libertad auténtica digital basada en la teoría liberal de F.A. Hayek.

Introducción

“La tecnología no es ni buena, ni mala, ni neutral”.

(Kranzberg 1986, p. 545)

El invento de Internet es de las creaciones más importantes en la historia de la humanidad. Una red de conexión que utiliza más de la mitad de la población mundial¹ y que destaca por ser más que una herramienta de comunicación. A diferencia del teléfono, la radio y la televisión, Internet es interoperable y permite la colaboración a escalas jamás vistas. Hoy en día somos una amalgama entre lo virtual y lo real. Mi ‘yo’ verdadero ahora es verificado a través de Google y Facebook, creando un vínculo íntimo entre mi acción externa y mi acción digital.

¹ “Internet used by 3.2 billion people in 2015”, <https://www.bbc.com/news/technology-32884867>, *BBC News*, 26 de mayo, 2015.

Vivimos en tiempos revolucionarios. Desde la comodidad de mi casa puedo enviar un correo a mi profesor, mientras escucho podcasts en YouTube de un creativo en Los Ángeles y compro algún producto de Alemania a través de Amazon. Esta interoperabilidad que no reconoce ninguna frontera geopolítica es el resultado del ingenio humano. No solo eso, pero también refleja la diversidad de interacción humana a escala digital.

Internet es la plataforma del ciberespacio, en el cual existen múltiples arquitecturas de conexión. A pesar de que Internet es global e indiferente a los límites geopolíticos, no es lo mismo hablar del Internet en China, E.E.U.U. o la Unión Europea, debido a las regulaciones internas de cada sector. A su vez, no es lo mismo hablar de criptomonedas, la *dark web* o las redes sociales. En Internet yacen múltiples realidades y cada una es de interés para comprender la complejidad de la acción humana en su ámbito digital.

El florecimiento del comercio y la comunicación en la red nos da a entender que el ciberespacio es merecedor de un análisis crítico en cuanto a su impacto en la condición humana. La acción individual ya no está limitada a su entorno físico y puede manifestarse de forma virtual. El activismo social, el comercio, la intimidad personal y el flujo libre de información ahora están a la distancia de un clic.

Por esto mismo, para comprender nuestra acción digital, es necesario analizar en qué esferas se está generando. Como punto de interés, este ensayo se enfocará en las redes sociales de occidente² por su alcance de población (por ejemplo, en el 2017 se reportaron 2.13 miles de millones de usuarios en Facebook alrededor del mundo³) y su rol como plataforma que promueve la democracia y la conexión humana.

Cuando se habla de democracia política en las redes sociales, se habla de la democratización de la comunicación masiva. Ahora, los usuarios pueden “retar los monopolios de la producción

² Esta investigación utiliza de referencias las redes sociales más populares en los Estados Unidos de acuerdo a la última investigación realizada por Pew Research Center. Se menciona a Facebook por ser la red social más popular con más usuarios en el momento de escribir esta investigación. Otras redes sociales notables en el occidente son: Twitter, LinkedIn, YouTube, Instagram, Pinterest y Snapchat. Es importante notar que existen otras redes sociales populares que funcionan fuera de la esfera occidental como VK en Rusia y WeChat en China.

³ Kirkpatrick, David, 2018:42.

y diseminación de medios por el Estado e instituciones comerciales”⁴. Por esto mismo, las redes sociales como Facebook son plataformas que promueven la participación política.

Un ejemplo claro de la capacidad de las redes sociales en crear un impacto político son las manifestaciones del mundo árabe del 2010 a 2013, también conocidas como Primavera Árabe. Otros ejemplos de movimientos sociopolíticos son *#BlackLivesMatter* y *Occupy Wall Street* en Estados Unidos, el movimiento 15-M en España y *#RenunciaYa*⁵ en Guatemala, los cuales ejemplifican que la acción digital tiene repercusiones en contextos fuera de lo virtual⁶.

A pesar de ser plataformas de comunicación y coordinación masiva con impacto político, es imperativo comprender que las redes sociales no son utilidades públicas. Facebook es una empresa privada y no hay ganancia en lo gratuito. El precio de mercado para usar las redes sociales no es monetario sino informático. Parte de la misión de este ensayo es indagar cómo la manera de generar ingresos en las redes sociales afecta el estado de libertad de los individuos en su esfera digital.

Capitalismo informático & Big Data

Las redes sociales se pueden definir como una agrupación de aplicaciones digitales basadas en fundamentos ideológicos y tecnológicos que permiten la diseminación y creación de contenido generado por usuarios⁷. En un inicio, estas plataformas eran percibidas como portadoras neutras de información entre usuarios, pero esta percepción ha cambiado debido a que las redes sociales ahora ofrecen servicios personalizados⁸. ¿Cómo se logra esta personalización? A través de la reducción de la socialización y las relaciones humanas en algoritmos para poder diseminar información de la manera más eficiente.

⁴ Loader & Mercea, 2012, traducido por la autora.

⁵ Torres, Gabriela, “How a peaceful protests changed a violent country”, <https://www.bbc.com/news/blogs-trending-32882520>, *BBC News*, 27 de mayo 2015.

⁶ De Choudhury, et al, 2016:92.

⁷ Kaplan & Haelein, 2010:60.

⁸ Djick, 2013:6.

Esta capacidad de personalización más el poder adquisitivo de las redes sociales a gran escala yacen en su capacidad de capturar la información generada por los usuarios que se conoce comúnmente como *Big Data* o datos masivos. Dana Boyd y Kate Crawford, en su artículo “Critical Question for Big Data” (2012), definen *Big Data* de la siguiente manera:

We define Big Data as a cultural, technological, and scholarly phenomenon that rests on the interplay of:

(1) Technology: maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets.

(2) Analysis: drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims.

(3) Mythology: the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy⁹.

Hay autores como West que definen a esta estructura de ingresos basada en la recolección de datos masivos como capitalismo informático en el cual, “el poder de las redes está en la creación de valor a partir de los pasos digitales producidos dentro de ellas mismas”¹⁰. Los datos de los usuarios son capturados, procesados y vendidos a terceros interesados en utilizar esa información, ya sea para marketing u otros fines como la propaganda o el proselitismo ideológico.

⁹ Boyd & Crawford, 2012: 663.

¹⁰ West, 2017:2.

Por esto mismo, la adquisición de *Big Data* requiere de una vigilancia constante, profunda y rigurosa, todo bajo un consentimiento ambiguo de los usuarios (más adelante se discutirá las fallas de los términos de uso en estas plataformas). Como explica Djick, las redes sociales pueden generar “empoderamiento intenso y explotación inquietante al mismo tiempo”¹¹.

Otro análisis del capitalismo informático viene de Shoshana Zuboff, quien es pionera en el análisis del capitalismo en su ámbito digital y desarrolló el término capitalismo de vigilancia. Si la acumulación de datos es necesaria en el capitalismo informático, entonces se requiere de una vigilancia para adquirir esta información. En su ensayo, “Big other: surveillance capitalism and the prospects of an information civilization” (2015), Zuboff explica que su misión es,

(...) to identify and theorize the currently institutionalizing logic of accumulation that produces hyperscale assemblages of objective and subjective data about individuals and their habitats for the purposes of knowing, controlling, and modifying behavior to produce new varieties of commodification, monetization, and control¹².

Como explica Zuboff, la lógica de agregación da lugar a plataformas que son diseñadas para modificar la conducta de los usuarios para seguir otorgando esos bienes. La crítica de Zuboff respecto al capitalismo de vigilancia es sumamente interesante y controversial, pero lo que no se puede negar en cuanto a las redes sociales es su capacidad de influenciar la conducta de sus usuarios.

Por ejemplo, Karen Yeung en su artículo “‘Hypernudge’: Big Data as a mode of regulation by design” (2017), explora la idea de un *hypernudge*, tomando prestado la idea de *nudge* de Thaler & Sustein (2008).

¹¹ Djick 2013:18, traducido por la autora.

¹² Zuboff, 2015:86.

By relying on the use of ‘nudge’, a particular form of choice architecture that alters people’s behaviour in a predictable way without forbidding any options or significantly changing their economic incentives, these techniques constitute a ‘soft’ form of design-based control¹³.

Yeung hace una genial analogía en la que explica que *nudge* sería poner un reductor de velocidad en alguna carretera; sin embargo, *hypernudge* tiene repercusiones mucho más profundas. Por ejemplo, en Facebook “el usuario promedio tiene acceso a 1,500 posts diarios, pero solo mira 300”¹⁴. Facebook determina qué es relevante para el usuario y crea una experiencia personalizada. En este caso, Facebook tiene el *poder* de estructurar las circunstancias digitales en las cuales se desarrollan los individuos¹⁵.

Otra consecuencia de la existencia de los datos masivos es que puede crear la ilusión de un conocimiento profundo sobre la condición humana. Las redes sociales pueden caer en un juego de ingeniería social donde la conducta de los usuarios es meticulosamente analizada para poder plantear un diseño o producto personalizado. El simple término de “personalizado” asume tener el conocimiento para saber anticipadamente qué es lo que busca una persona *incluso antes que ella misma lo determine*.

En efecto, es realmente preocupante ver la escala de vigilancia que tienen las redes sociales sobre sus usuarios y la ausencia de transparencia en la utilización de esos datos. Los algoritmos que dictan las circunstancias de nuestras interacciones digitales son considerados

¹³ Yeung 2016: 118.

¹⁴ Yeung, 2017:130, traducido por la autora.

¹⁵ Las redes sociales ahora juegan un rol importante en los procesos electorales y también son plataformas de difusión para las *fake news* o noticias falsas. Todavía no se ha respondido concretamente la pregunta, ¿qué tanto influyen las redes sociales el voto político? Es imperativo reconocer el rol de las redes sociales en la difusión de desinformación. Para más información, se recomienda investigar sobre el Brexit, la campaña política de Obama, Trump o Bolsonaro.

*trade-secrets*¹⁶, solamente disponibles para las corporaciones o gobiernos, lo cual les otorga un monopolio en la capacidad de influenciar la conducta digital de los usuarios.

Aún más importante parece ser la observación de que esta vigilancia no se extiende solamente a las entidades privadas. Más adelante se analizará la situación de Estados Unidos, en la que ha habido instancias en las cuales el gobierno ha podido interceptar cierta información privada. *Scientia potentia est* y no debería de sorprendernos que haya intentos constantes por ejercer vigilancia gubernamental sobre las redes sociales.

Estas observaciones, más que nada, son aquellas que me inspiran a implementar las ideas liberales en el ámbito digital. Considero imperativo realizar un rescate de la tradición liberal en el ciberespacio para poder deliberar, ¿qué tipo de red social queremos?

Libertad digital

La libertad que será explorada es la de la tradición liberal hayekiana. Esto significa que al hablar de “libertad” se habla de la ausencia de coerción arbitraria por parte de terceros y no del estado de poder hacer lo que uno quiera sin consecuencias. Notemos esta diferencia para poder apreciar cómo sí se podría lograr un estado de libertad digital y cómo el modelo actual de las redes sociales impide esta libertad auténtica por múltiples razones.

¿Cómo nos podemos imaginar una libertad auténtica en el ámbito digital? Argumento que se requiere una esfera privada lejos de la vigilancia para poder complementar la esfera de responsabilidad en los individuos. Otro, es transparencia en la utilización de datos para dar a entender en qué circunstancias se encuentran los usuarios. Y el último es tener asegurada la protección de mi privacidad a través de la discreción y tener certeza de que mi información no está siendo sometida a una vigilancia ilegítima.

¹⁶ West, 2017:13.

1. Esfera de responsabilidad digital

Uno de los problemas primordiales que existe en Internet es, ¿cómo podemos verificar la identidad de las personas en su ámbito digital? Esta pregunta es clave para poder desarrollar una defensa de la libertad auténtica. El verdadero individualismo, como lo propone Hayek, no recae en su capacidad de evadir la ley y hacer lo que se quiera sin consecuencia. Todo lo contrario, para poder desarrollar una libertad auténtica se requiere de una esfera de responsabilidad¹⁷.

En su libro, *Code 2.0* (2005), Lawrence Lessig reflexiona sobre la verificación de identidad en medios digitales para poder crear un Estado de derecho virtual. Primero, no se puede ejercer la ley sobre un sujeto que no existe. La diferencia clave entre los sujetos virtuales y análogos es que las identidades en el mundo virtual son construidas. Hay aspectos de nuestra identidad que son otorgados de manera implícita en espacios reales, por ejemplo, el color pelo, el sonido de nuestra voz o nuestra altura. Esto se diferencia de Internet, en el cual es necesario que esa información sea explícitamente descrita.

Las redes sociales como Facebook tienen un gran incentivo para conseguir la información real de sus usuarios. Cuanto más auténtica sea la información que consiga, mejor será para las personas interesadas en utilizarla. Los usuarios también tienen un buen incentivo para usar su verdadero nombre en LinkedIn y Facebook, pues son plataformas de redes de contactos que mantienen usuarios contactados. De esta manera, las redes sociales se vuelven las credenciales informales de nuestra presencia digital.

No solo eso, las redes sociales ahora son utilizadas por instituciones y entidades privadas para hacer una verificación de antecedentes de sus futuros empleados y estudiantes¹⁸. Esto genera

¹⁷ Hayek, 1974:18.

¹⁸ Bell, Melissa, "More employers using firms that check applicants' social media history", https://www.washingtonpost.com/lifestyle/style/more-employers-using-firms-that-check-applicants-social-media-history/2011/07/12/gIQAxnJYGI_story.html?utm_term=.493442723107, *Washington Post*, consultado el 1 de septiembre, 2018.

que los usuarios sean más cautelosos en su comportamiento digital que tiene repercusiones en su identidad análoga¹⁹.

Lo que hay que evitar cuando se habla de una libertad auténtica digital es querer remover la esfera de responsabilidad de los individuos. Es imperativo mantener las circunstancias adecuadas para que la ley pueda ser ejercitada y el anonimato es el camino seguro para perder un Estado de derecho virtual.

2. Términos de uso y normas de conducta

Los términos de uso en las redes sociales son las normas de convivencia. Aun así, existe un gran problema que los términos de uso deben superar: nadie las lee y están sometidas a cambios constantes. Por ejemplo, un estudio realizado por York University y Connecticut University demostró que la gente no lee los términos de privacidad y servicio. El estudio utilizó una variante de los términos de uso de la red social LinkedIn y agregaron una cláusula en la cual los participantes pactaron en darle su primer hijo como pago. En total, el 98% de los participantes no se percataron de esta cláusula en el contrato²⁰.

Para que pueda desarrollarse un Estado de derecho digital, los usuarios deben de estar enterados de las normas que regulan su conducta. Por el momento, los términos de uso son de naturaleza positivas e inestables y, por ende, no son un buen marco para la libertad auténtica. Tomemos el análisis de Hayek: “Las normas, que están para servir como guías a los individuos en sus propios planes, deberían ser concebidas para regir por períodos largos”²¹.

¹⁹ Es sumamente interesante analizar las normas de conducta análogas que influyen la conducta digital. Por ejemplo, los movimientos de justicia social manejan una agenda de censura y castigo para los infames discursos de odio. Es necesario tener una conversación crítica sobre qué es una transgresión a la ley en el ámbito virtual para evitar el abuso del poder y el conocimiento.

²⁰ Obar & Oeldorf-Hirsch, 2018:2.

²¹ Hayek, 1974:18.

Los términos de uso han caído en la trampa de la legislación positiva donde solamente los expertos saben qué está sucediendo. Los individuos no pueden ejercer decisiones informadas si no comprenden la ley que los rodea. El problema actual de los términos de uso en las redes sociales es que no son amigables o comprensibles para el público general. La FTC de los Estados Unidos realizó una investigación sobre el lenguaje en los términos de uso y determinó que son confusos y contradictorios²². Asimismo, solo porque un servicio tiene reglas sobre la privacidad no significa que su misión sea la preservación de esa privacidad.

El individuo necesita comprender qué derechos tiene asegurados para poder reclamarlos. Un ejemplo puede observarse después del escándalo en torno a Cambridge Analytica, en el cual la gente exigió una respuesta de Mark Zuckerberg (CEO de Facebook) después de una fuga masiva de información personal en el cual aproximadamente 87 millones de usuarios fueron afectados. Solo al tener una idea clara de qué es lo que tiene asegurado el individuo, este puede hacer alguna denuncia cuando esos límites se transgreden.

Los términos de uso tienen una gran falla: la ineficiencia de comunicar las normas de conducta de manera clara. Una posible solución a este problema es tener una declaración de intenciones y una lectura de normas que promuevan la libertad negativa, es decir, la ausencia de la interferencia de otros.

3. Vigilancia legítima e ilegítima

La convivencia en paz en sociedad conlleva que haya una vigilancia legítima de nuestras acciones. La vigilancia no es mala siempre y cuando ocurra bajo el conocimiento de los usuarios vigilados. Hoy en día acordamos a ser observados por cámaras de seguridad, velocímetros y la mirada de otros. Una buena sociedad tiene vigilancia para conseguir que los individuos sean responsables de sus acciones.

²² FTC, 2000:24.

En el mundo virtual también hay un uso legítimo de la vigilancia. Por ejemplo, las *cookies* son herramientas de rastreo que facilitan nuestro uso de las páginas web. Una *cookie* es un archivo pequeño que envía un servidor web al disco duro del internauta que lo visita con información sobre sus preferencias y pautas de navegación²³. Las cookies les otorgan a las páginas web la capacidad de recordar quienes somos y si ya hemos visitado su página anteriormente. Por ejemplo, si hemos introducido nuestro usuario y contraseña. De esta manera, las *cookies* les dan a los usuarios una ventaja para navegar la web.

El problema empieza cuando los individuos están siendo sometidos a una vigilancia ilegítima que otorga información sensible que puede ser utilizada para los fines de otros. Una instancia nefasta en cuanto al abuso de poder estatal para realizar esta vigilancia es la USA *PATRIOT Act* (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001).

En el 2001, durante la presidencia de Bush, en Estados Unidos se aprobó la ley federal patriótica conocida comúnmente como *PATRIOT Act*. Tal como lo indica en su acrónimo, esta ley tiene como fin unir y fortalecer los Estados Unidos proveyendo las herramientas apropiadas para impedir y obstaculizar el terrorismo. Esta ley fue aprobada como una respuesta a los ataques terroristas del 11 de septiembre de 2001 y le otorgó al gobierno de Estados Unidos la capacidad de realizar investigaciones secretas sin el conocimiento de los sujetos²⁴.

Lo que era considerado una medida de precaución necesaria, rápidamente colapsó bajo las revelaciones de Edward Snowden en el 2013²⁵. El exagente de la CIA reveló que los ciudadanos de Estados Unidos estaban siendo sometidos a una vigilancia masiva sin su conocimiento.

²³ Definición prestada de Google, consultada el 12 de julio, 2018.

²⁴ Rubel, 2005:1.

²⁵ Otro personaje que resalta por sus aportes al ciberactivismo es Julian Assange, el fundador de Wikileaks. El ciberactivismo ocurre cuando un individuo hace pública información confidencial. Wikileaks es una página web sin fines de lucro que publica información sensible, fugas de noticias y medios clasificados suministrados por fuentes anónimas. Existe un debate en torno a este tipo de activismo y la justificación moral detrás de ella.

Por ejemplo, el gobierno de los Estados Unidos demandó²⁶ de Verizon (una empresa de telecomunicaciones privada) un registro absoluto de sus usuarios sin la capacidad de informar a sus clientes que estaban siendo vigilados de manera ilegítima. No existe un ejemplo más claro del abuso de poder estatal para ejercer coerción sobre las empresas privadas para utilizarlas como un medio de vigilancia masiva²⁷.

Hayek defiende que no hay libertad si el individuo no tiene una esfera privada. "Freedom thus presupposes that the individual has some assured private sphere, that there is some set of circumstances in his environment with which others cannot interfere"²⁸.

Por esto, la vigilancia ilegítima disminuye la libertad auténtica que puede suceder en las redes sociales. Al no saber quién está vigilando y el alcance de esta vigilancia, los usuarios pueden empezar a censurar sus acciones por miedo a repercusiones. Eso, acumulado con términos de uso difíciles de comprender, dan como resultado espacios perfectos para el abuso del conocimiento.

Desde un inicio, se exploró los aspectos negativos del anonimato en cuanto a la esfera de responsabilidad de los individuos, pero se requiere un rescate a los aspectos positivos del anonimato en cuanto a la resistencia de la vigilancia ilegítima. En vez de pensar en el anonimato, se podría hablar del valor de la reclusión: estar lejos de la vista de otros²⁹. El anonimato puede ser utilizado como herramienta de resistencia a la vigilancia ilegítima y también como un método para señalar abusos de poder y diseminar información que pone en riesgo a los testigos (como en el caso de Edward Snowden).

²⁶ Orden judicial de Verizon: <https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order>

²⁷ Otro ejemplo notable del abuso de poder Estatal yace en China, donde el gobierno censura y vigila sus ciudadanos a través de redes sociales y reconocimiento facial. Incluso ha desarrollado un sistema de punteo social donde clasifican a la población de acuerdo a los estándares de conducta elegidos por el gobierno.

²⁸ F.A. Hayek, 1960:61.

²⁹ Levmore & Nussbaum, 2011:10.

Hay que diferenciar ser público de estar en público³⁰ y es importante empezar a reconocer que la única forma de complementar la esfera de responsabilidad de los individuos es otorgándoles a los usuarios un espacio privado lejos de la posibilidad de una vigilancia ilegítima y de una interferencia por parte de terceros.

Conclusiones

La misión de este ensayo fue explorar el estado de la libertad individual en las redes sociales. El desenlace de este punto de investigación yace en que la libertad individual está amenazada por tres puntos: la ausencia de la esfera privada, la existencia de manipulación de circunstancias y la amenaza constante de vigilancia ilegítima. Para ser plataformas que declaran ‘conectar gente’ parece que hay una gran desconexión de la necesidad más básica: la libertad.

La utilidad de las redes sociales yace en los motivos personales de cada usuario. En sí, las redes sociales como herramientas de comunicación no son buenas, ni malas, pero tampoco son neutras. Por esto, es importante revisar las filosofías que gobiernan las arquitecturas que forman nuestra acción digital. Podemos celebrar los avances tecnológicos y ser críticos al respecto. Es un peligro caer en la idea de que toda mejora tecnológica es progreso. Por lo tanto, Internet y las redes sociales requieren una constante crítica que debería tener como misión la preservación de la libertad individual.

Debido a esto, a pesar de que las redes sociales son entidades privadas, debemos de ser críticos sobre su conducta y la política que dicta sus acciones. Las redes sociales han democratizado la comunicación masiva pero no son utilidades públicas³¹. Considerando esto, actitudes como la ingeniería social y la venta masiva de información privada deben de ser cuestionadas. Otorgarle a un par de corporaciones la información necesaria para influenciar nuestra conducta digital ha de preocuparnos.

³⁰ Boyd & Crawford, 2012:13.

³¹ Es necesario revisar la literatura en cuanto a la diferencia entre una utilidad pública y un servicio privado.

Otro punto de reflexión es comprender que las corporaciones y las empresas privadas no son inmunes a la corrupción moral. La centralización de información les da a selectas redes sociales el poder de influenciar la conducta de sus usuarios. La posibilidad de que nuestras circunstancias sean modificadas sin nuestro conocimiento es una manera asegurada de perder nuestra libertad auténtica. Sin duda, es importante que las personas tengan un uso de conocimiento adecuado para poder aceptar esas condiciones. El otro problema es que la forma de redacción de los términos de uso no es eficiente en su misión, la cual es explicar las circunstancias en las cuales se encuentran los usuarios.

Notemos que esto tampoco es un argumento a favor de la regulación de las redes sociales. Cuando se trata de servicios privados, el mejor voto es con los pies. No hay que regular las diversas redes sociales como Facebook, Twitter, LinkedIn, Instagram o Snapchat, pues aquellas pueden ser reemplazadas por otras redes sociales. Por ejemplo, MySpace, Vine y Hi5 eran plataformas sumamente populares y ahora han caído en el olvido. Es más importante revisar las prácticas de comercio y las filosofías que impulsan estas plataformas que crear regulaciones.

Otra preocupación central, en cuanto a las prácticas de las redes sociales, es la amenaza de la ingeniería social. Con respecto a *Big Data* es importante involucrar a los académicos de las ciencias sociales. La vigilancia continua y la adquisición en cantidades masivas de información sobre los individuos puede generar un falso conocimiento del hombre. No hay que descuidar la importancia de las instituciones y las ideas de libertad que se han desarrollado a través de los siglos, pues corremos el riesgo de caer en la trampa de la razón pura, el positivismo científico.

Reconocer en las redes sociales su naturaleza de influencia en la conducta de los individuos es imprescindible para entender las posibles respuestas. Las redes sociales son el resultado de una demanda en el mercado y son construcciones artificiales. Por esto mismo, tenemos la

oportunidad de crear alternativas que respeten nuestra libertad negativa. Nosotros podemos decidir qué tipo de red social queremos, o el uso específico que le damos.

Aún más imperativo es lograr una alfabetización digital al lado de una concientización en cuanto a la conducta virtual. Al establecer que nuestra acción digital y análoga están íntimamente vinculadas, es necesario comprender las circunstancias que gobiernan esos espacios. Hay usuarios que están renunciando a su esfera privada a fin de poder utilizar servicios que aparentan ser gratuitos sin conocer el verdadero trasfondo de su decisión. En definitiva, son servicios que se compran facilitando información personal y atención a espacios con publicidad de anunciantes.

Por ejemplo, Pew Research Center realizó un estudio de la perspectiva general³² de las redes sociales entre jóvenes de 13 a 17 años. Después de estudiar la opinión de más de 1,000 adolescentes se concluyó que el 76% utiliza alguna red social (Facebook era la más popular en 2015) y se reporta que el 92% de adolescentes se conectan en línea todos los días. Por esto, es importante difundir una noción general de *cómo* funcionan las redes sociales para tener un uso de conocimiento adecuado.

Sin duda, esta investigación es la punta del iceberg. Dentro de este marco, solamente se exploró una libertad en base a las ideas de Hayek. Todavía se requiere un análisis más extenso de la tradición liberal en el ámbito digital. También, se requiere de una sensibilización a la noción de la interacción humana. Por su naturaleza, las redes son un constructo artificial, pero la interacción humana no se puede diseñar. Lo único natural de las redes sociales son las personas que lo utilizan, por ende, es de gran interés tratar de crear circunstancias en las cuales ellas se puedan desenvolver de la manera más plena y libre.

³² Pew Reserch Center, "Teens, Social Media, & Technology Overview 2015: Smartphones facilitate shifts in communication landscape for teens", http://www.pewinternet.org/files/2015/04/PI_TeensandTech_Update2015_0409151.pdf#3, consultado el 14 de julio, 2018.

Es momento de otorgar a la libertad el protagonismo que requiere en las esferas virtuales. Como cibernautas, tenemos la responsabilidad de velar por la libertad y demandar un cambio sobre aquello que no lo asegura. Como diría Hayek, no existe la libertad sin la responsabilidad y es momento de que se genere más conversaciones en torno a la situación actual de la libertad en su esfera digital.

Bibliografía:

- Brian D. Loader, Dan Mercea, *Social Media and Democracy: Innovations in Participatory Politics*, Routledge, Nueva York, 2012.
- De Choudhury, M., Jhaver, S., Sugar, B., & Weber, I., "Social Media Participation in an Activist Movement for Racial Equality", *International AAAI Conference on Weblogs and Social Media*, 2016, 92–101.
- Dencik, L., Hintz, A. and Cable, J., "Towards data justice? The ambiguity of anti-surveillance resistance in political activism", *Big Data & Society*, vol. 3(2), 2016, 1 -12.
- Edwards, Haley Sweetland. "The Masters of Mind Control", *Time*, vol. 191, (15), 2018, 30-37.
- Fidler, David P., *The Snowden Reader*. Indiana University Press, Estados Unidos, 2015.
- Hayek, F. A, *Constitution of Liberty*. University of Chicago Press, Chicago, 1960.
- Hayek, F.A, *La fatal arrogancia: los errores del socialismo*, Unión Editorial, Madrid, 1990.
- Hayek, F. A, "Individualismo: el verdadero y el falso", *Estudios Públicos*, vol. 0(12), 1974, 28.
- Kaplan, A. M., & M. Haenlein. "Users of the world, unite! The challenges and opportunities of social media", *Business Horizons*, vol. 53(1), 2010, 59–68.
- Kirkpatrick, D. "The Facebook Defect", *Time*, vol. 191(15), 2018, 38-44.
- Lessig, L, *Code. 2nd ed.* Basic Books, Nueva York, 2006.
- Obar, Jonathan A. and Oeldorf-Hirsch, Anne, "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services", *Information, Communication & Society*, 2018, 1-20.
- Rubel, Alan, "Privacy and the USA Patriot Act: Rights, the Value of Right, and Autonomy", *Law and Philosophy*, vol. 26(2), 2007, 119-159.
- Saul Levmore, Martha C. Nussbaum, *The Offensive Internet: Speech, Privacy, and Reputation*, Harvard University Press, Cambridge, 2010.

Silverman, J., *Terms of Service: Social Media and the Price of Constant Connection*.

HarperCollins, Nueva York, 2015.

Sprenger, F., *The Politics of Micro-Decisions: Edward Snowden, Net Neutrality, and the Architectures of the Internet*. Milton Keynes, Lightning Source, 2015.

Steinmetz, K., "Can Congress Reign In Big Tech?", *Time*, vol. 191(15), 2018, 46 - 47.

Taddeo, Mariarosaria, "The Struggle Between Liberties and Authorities in the Information Age", *Science and Engineering Ethics*, vol. 21(5), 2015, 1125–1138.

United States, Congress, Federal Trade Commission, *Privacy Online: Fair Information Practices in The Electronic Marketplace*, Washington, 2000.

West, Sarah Myers. "Data Capitalism: Redefining the Logics of Surveillance and Privacy", *Business & Society*, 0(0), 2017.

Yeung, Karen, "'Hypernudge': Big Data as a mode of regulation by design", *Information, Communication & Society*, vol. 20(1), 2017, 118-136.

Zuboff, Shoshana, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization", *Journal of Information Technology*, vol. 30(1), 2015, 75–89.